Bosch IP video products

ru Руководство по кибербезопасности

Содержание

1 Назначение документа и целевая аудитория

Технологии развиваются очень быстро, иногда с по-настоящему головокружительной скоростью. Стремительное развитие искусственного интеллекта (ИИ) и Интернета вещей (IoT), а также их массовое применение (AIoT) изменили профиль рисков для продуктов и сервисов. Атаки злоумышленников становятся более распространенными и легкоосуществимыми ввиду все более широкого внедрения технологий подключения. Поэтому предоставление безопасных и надежных продуктов и сервисов заказчикам является целью компании Bosch.

Это руководство предназначено для помощи интеграторам в усилении систем IP-видеонаблюдения от Bosch с целью достижения более полного соответствия существующим правилам и процедурам сетевой безопасности их клиентов.

В настоящем руководстве рассматриваются следующие вопросы:
- Важнейшая информация о функциях и основных характеристиках IP-видеоустройств Bosch
- Конкретные функции, которые можно изменять или отключать
- Конкретные функции, которые можно активировать и использовать
- Передовые методики, относящиеся к видеосистемам и безопасности

Основное внимание в настоящем руководстве уделено использованию Configuration Manager для выполнения указанных конфигураций. В большинстве случаев все конфигурации можно выполнить с использованием системы BVMS, клиента Configuration Client, Configuration Manager и встроенного веб-интерфейса видеоустройства.

2 Концепция безопасности и меры предосторожности

IP-видеоустройства становятся все более распространенными в современной сетевой среде, и, как и при наличии любых других IP-устройств в сети, при использовании этих устройств IP-администраторы и сотрудники службы безопасности имеют право знать всю полноту набора функций и возможностей устройства.

При использовании IP-видеоустройств Bosch первым уровнем вашей защиты являются сами устройства. Кодеры и камеры Bosch производятся в контролируемых и безопасных условиях и проходят постоянные проверки. Запись программы в устройства может производиться только с помощью загрузки корректной микропрограммы, разработанной специально для серии оборудования и набора микросхем.

Большинство IP-видеоустройств Bosch поставляется со встроенным чипом безопасности, обеспечивающим функции, аналогичные функциям криптомикропроцессора и так называемого Trusted Platform Module, сокращенно модуля TPM. Этот чип выступает в качестве сейфа для важнейших данных; он защищает сертификаты, пароли, лицензии и т.д. от несанкционированного доступа, даже если камера подвергается физическому вскрытию с целью получения доступа.

IP-видеоустройства Bosch прошли более чем тридцать тысяч (30000) проверок на уязвимость и возможность проникновения, проведенных независимыми поставщиками продуктов безопасности. На сегодняшний день не произошло еще ни одной успешной кибератаки на должным образом защищенное устройство.

3 Безопасная установка

3.1 Серверы и устройства хранения

Все компоненты серверов (например BVMS Management Server и сервер Video Recording Manager), а также устройства хранения должны быть установлены в защищенной области. Доступ к защищенной области должен обеспечиваться через систему управления доступом и контролироваться. Группа пользователей, которая имеет доступ к центральному серверному помещению, должна быть ограничена небольшим количеством лиц.
Даже если серверы и устройства хранения установлены в защищенной области, необходимо обеспечить их защиту от несанкционированного доступа.

См.

- *Усиление безопасности серверов, Страница 34*
- *Повышение уровня безопасности хранилищ, Страница 33*

3.2 Камеры и периферийные устройства

При монтаже камер и периферийных устройств нужно выбрать безопасное расположение и ориентацию установки. Наилучшим расположением является такое, где устройство не будет подвергаться умышленным или случайным воздействиям.

4 Безопасная конфигурация

4.1 Назначение IP-адресов

Все IP-видеоустройства Bosch в настоящее время поставляются с заводскими настройками, позволяющими назначить IP-адрес DHCP.
При отсутствии доступного сервера DHCP в активной сети, в которой размещено устройство, устройство — если на нем установлена микропрограмма версии 6.32 или новее — автоматически назначит link-local адрес из диапазона 169.254.1.0 — 169.254.254.255, или 169.254.0.0/16.
В случае более ранних версий микропрограммы оно самостоятельно назначит себе IP-адрес по умолчанию 192.168.0.1.
Существует несколько инструментов назначения IP-адресов IP-видеоустройствам Bosch, в том числе:

- Bosch Configuration Manager
- BVMS Configuration Client
- BVMS Configuration Wizard

Все инструменты ПО поддерживают функцию назначения единого статического адреса IPv4, а также диапазона адресов IPv4 нескольким устройствам одновременно. Это включает маску подсети и назначение адресов шлюзам по умолчанию.
Все адреса IPv4 и значения маски подсети должны быть введены в так называемом «десятичном представлении с точками».

Замечание!
Одной из первостепенных мер по ограничению возможностей внешних кибератак на систему, осуществляемых несанкционированными локально подключенными сетевыми устройствами, является ограничение числа доступных неиспользуемых IP-адресов. Это можно сделать с помощью IPAM (**IP A**ddress **M**anagement, управление IP-адресами), совместно с разбитием на подсети диапазона IP-адресов, который будет использоваться.

Разбитие на подсети — это процесс заимствования битов из хост-части IP-адреса с целью разбития большой сети на несколько малых. Чем больше таких битов заимствуется, тем больше сетей можно создать, но тем меньше адресов узлов каждая из сетей будет поддерживать.

Суффикс	Узлы	CIDR	Заимствованные	Двоичные
.255	1	/32	0	.11111111
.254	2	/31	1	.1111111**0**
.252	4	/30	2	.111111**00**
.248	8	/29	3	.11111**000**
.240	16	/28	4	.1111**0000**
.224	32	/27	5	.111**00000**
.192	64	/26	6	.11**000000**
.128	128	/25	7	.1**0000000**

С 1993 г. Рабочая группа проектирования Интернета (IETF) ввела новую концепцию размещения блоков адресов IPv4 способом более гибким, чем тот, что использовался ранее в архитектуре назначения адресов с использованием классов. Новый метод называется «Бесклассовой междоменной маршрутизацией» (CIDR) и используется также с адресами IPv6.

Классовые сети IPv4 делятся на классы A, B и C с числом сетевых битов 8, 16 и 24 соответственно, и класс D, используемый для групповой адресации.

Пример:
Чтобы привести простой для понимания пример, мы используем сценарий с адресом класса C. Маска подсети по умолчанию для адреса класса C — 255.255.255.0. В техническом отношении, эта маска не была разбита на подсети, так что весь последний октет доступен для действительной адресации узлов. Так как мы заимствуем биты с адреса узла, для нас доступны следующие варианты маски в последнем октете:
.128, .192, .224, .240, .248 и .252.

При использовании маски подсети 255.255.255.240 (4 бита) мы создаем 16 меньших сетей, поддерживающих 14 адресов узлов на подсеть.
- Идентификатор подсети 0:
  диапазон адресов узлов от 192.168.1.1 до 192.168.1.14. Широковещательный адрес 192.168.1.15
- Идентификатор подсети 16:
  диапазон адресов узлов от 192.168.1.17 до 192.168.1.30. Широковещательный адрес 192.168.1.31
- Идентификаторы подсети: 32, 64, 96, и т. п.

Для более крупных сетей может потребоваться следующий по размеру класс сети B или определение соответствующего блока CIDR.

Пример:
Перед развертыванием сети видеонаблюдения необходимо выполнить простой расчет необходимого количества IP-устройств в сети, чтобы обеспечить возможность для будущего расширения:
- 20 рабочих станций для видео
- 1 центральный сервер
- 1 сервер VRM
- 15 массивов хранения данных iSCSI
- 305 IP-камер

Итого = необходимо 342 IP-адреса

Учитывая рассчитанное количество IP-адресов, равное 342, для обеспечения такого количества адресов нам по минимуму требуется схема IP-адресов класса B. Использование маски подсети класса B по умолчанию 255.255.0.0 позволяет использовать в сети 65534 доступных IP-адреса.

Кроме того, сети можно планировать с помощью блока CIDR, где 23 бита используются как префикс, обеспечивая адресное пространство на 512 адресов, соответственно, 510 узлов.

Разбивая большую сеть на более мелкие составляющие, то есть на подсети, или определяя блок CIDR, вы можете снизить риск.

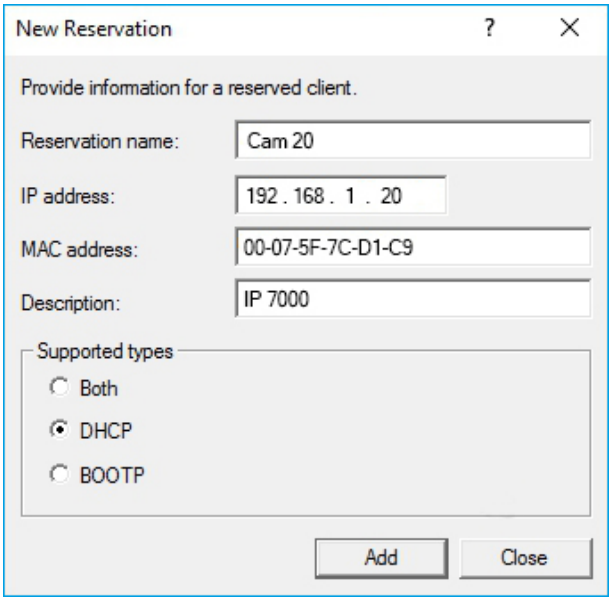
Пример:

	По умолчанию	**Разбито на подсети**
Диапазон IP-адресов	172.16.0.0 - 172.16.255.255	172.16.8.0 - 172.16.9.255
Маска подсети	255.255.0.0	255.255.254.0
Значение CIDR	172.16.0.0/16	172.16.8.0/23
Количество подсетей	1	128
Количество узлов	65.534	510
Избыточные адреса	65.192	168

4.1.1 Управление DHCP

IPAM может использовать DHCP в качестве мощного инструмента контроля и использования IP-адресов в вашей среде. DHCP можно настроить для использования конкретного набора IP-адресов. Его также можно настроить для исключения конкретного диапазона адресов.

Если вы используете DHCP, рекомендуется, при размещении видеоустройств, настроить бессрочное резервирование адреса на основе MAC-адреса каждого устройства.



Замечание!

Даже до использования управления IP-адресами для отслеживания использования IP-адресов, передовой методикой в управлении сетями является ограничение доступа к сети через безопасность портов на граничных коммутаторах, например, только конкретный MAC-адрес может получить доступ через конкретный порт.

4.2 Учетные записи и пароли пользователей

Все камеры и кодеры IP-видеонаблюдения Bosch поставляются с тремя встроенными учетными записями пользователя:

– **live (режим реального времени)**
  : эта стандартная учетная запись пользователя обеспечивает доступ к видеоизображению в режиме реального времени.
– **user (пользователь)**
  : эта расширенная учетная запись обеспечивает доступ к видео в режиме реального времени и видеозаписям, а также к такому управлению камерой, как управление PTZ. Данная учетная запись не предусматривает доступа к параметрам конфигурации.
– **service (служебная)**
  : эта учетная запись администратора обеспечивает доступ ко всем меню устройства и ко всем параметрам конфигурации.

Каждой учетной записи пользователя должен быть присвоен пароль.
Присвоение паролей является важнейшим этапом процесса защиты любого сетевого устройства. Настоятельно рекомендуется задать пароли для всех установленных сетевых видеоустройств.

Замечание!
В версии микропрограммы 6.30 управление пользователями было расширенно для большей гибкости и позволяет создавать других пользователей с именами пользователя и паролями. Бывшие уровни учетных записей теперь представляют уровни групп пользователей.
В версии микропрограммы 6.32 были введены более строгие требования к паролям (подробные сведения см. на странице *Назначение паролей с помощью веб-страницы устройства, Страница 12*).

4.2.1 Назначение паролей

Существует несколько способов назначения пароля в зависимости от размера системы видеонаблюдения и используемого ПО. В малых системах, состоящих из нескольких камер, пароли можно задать с использованием веб-страницы устройства или Bosch Configuration Manager, так как в нем удобно сочетаются функции одновременной конфигурации нескольких устройств и мастера конфигурации.

Замечание!
Как уже было сказано, пароли являются важнейшим элементом защиты данных от потенциальных кибератак. Это относится ко всем устройствам во всей вашей инфраструктуре безопасности. Большинство организаций уже имеют действующие строгие правила в отношении паролей, но если вы работаете с новой системой, не имея таких правил, рекомендуем вам ознакомиться с общепринятыми требованиями к защитным паролям:
— пароли должны быть от 8 до 12 символов длиной.
— пароли должны содержать буквы как верхнего, так и нижнего регистра.
— пароли должны содержать как минимум один специальный символ.
— пароли должны содержать как минимум одну цифру.

Пример:
Использование фразы «to be or not to be» и наших основных правил для создания надежного пароля.
– 2be0rnOt!t0Be

Замечание!
Существует ряд ограничений на использование в паролях таких специальных символов, как «@», «&», «<», «>», «:», в связи с их предписанным значением в XML и других языках разметки. Несмотря на то, что веб-интерфейс пропустит такие символы, другое ПО управления и конфигурирования может отказаться их принимать.

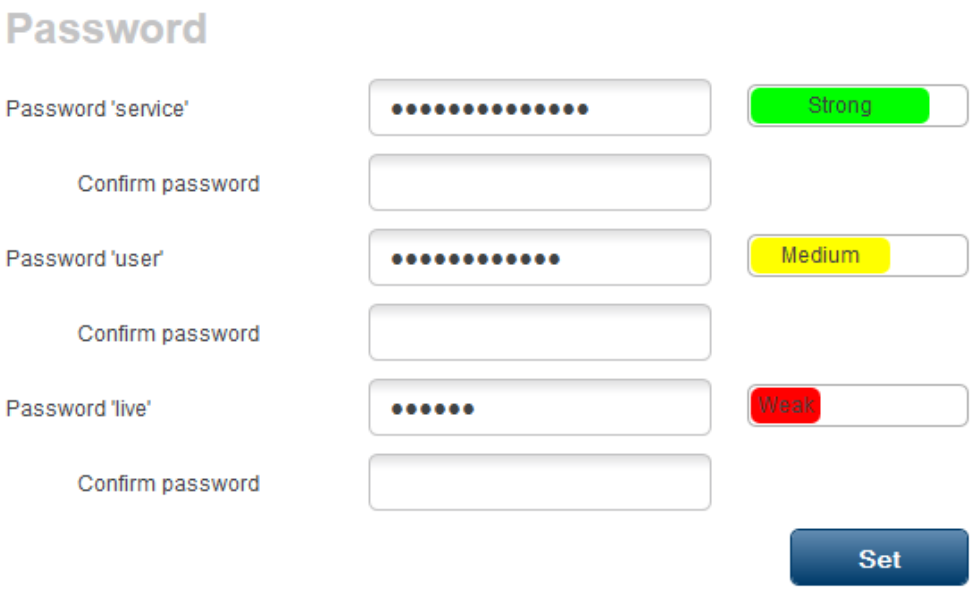
4.2.2 Назначение паролей с помощью веб-страницы устройства

1. На веб-странице устройства перейдите на страницу **Конфигурация**.
2. Выберите меню общих настроек **Общие** и подменю **Управление пользователями** (Примечание: до версии микропрограммы 6.30 подменю **Управление пользователями** называлось **Пароль**).

При первом переходе на веб-страницу камеры пользователю предлагается назначить пароль для обеспечения минимальной защиты.
Это предложение будет отображаться при каждом новом переходе на веб-страницы камеры до тех пор, пока пароль не будет задан. Нажатие кнопки **ОК** ведет к автоматическому открытию меню **Управление пользователями**.

В версии микропрограммы 6.30 есть возможность установки флажка **Не показывать...**. Эта возможность была исключена в версии микропрограммы 6.32 в целях избежания пробелов в безопасности.

1. Выберите меню **Управление пользователями** и введите и подтвердите пароли для каждой из трех учетных записей.
   Обратите внимание:
   - Сначала необходимо назначить пароли для наиболее высокого уровня доступа (**Пароль 'service'**).
   - В версии микропрограммы 6.20 и более поздних новый индикатор надежности пароля подскажет, насколько потенциально надежен введенный вами пароль. Это вспомогательный инструмент и он не гарантирует абсолютного соответствия введенного вами пароля требованиям безопасности конкретной установки.
2. Нажмите **Установить** для применения и сохранения изменений.



Страница **Управление пользователями** в версии микропрограммы 6.30 обеспечивает большую гибкость для создания пользователей с произвольными именами и собственными паролями. Бывшие уровни учетных записей теперь представляют уровни групп пользователей.

Стандартные пользователи продолжают существовать, используя пароли, заданные с помощью более ранней версии микропрограммы; их невозможно удалить, а также невозможно изменить уровень их группы.

Пароли можно задавать или изменять нажатием или  .
Пока все учетные записи не будут защищены паролями, будет отображаться предупреждающее сообщение.

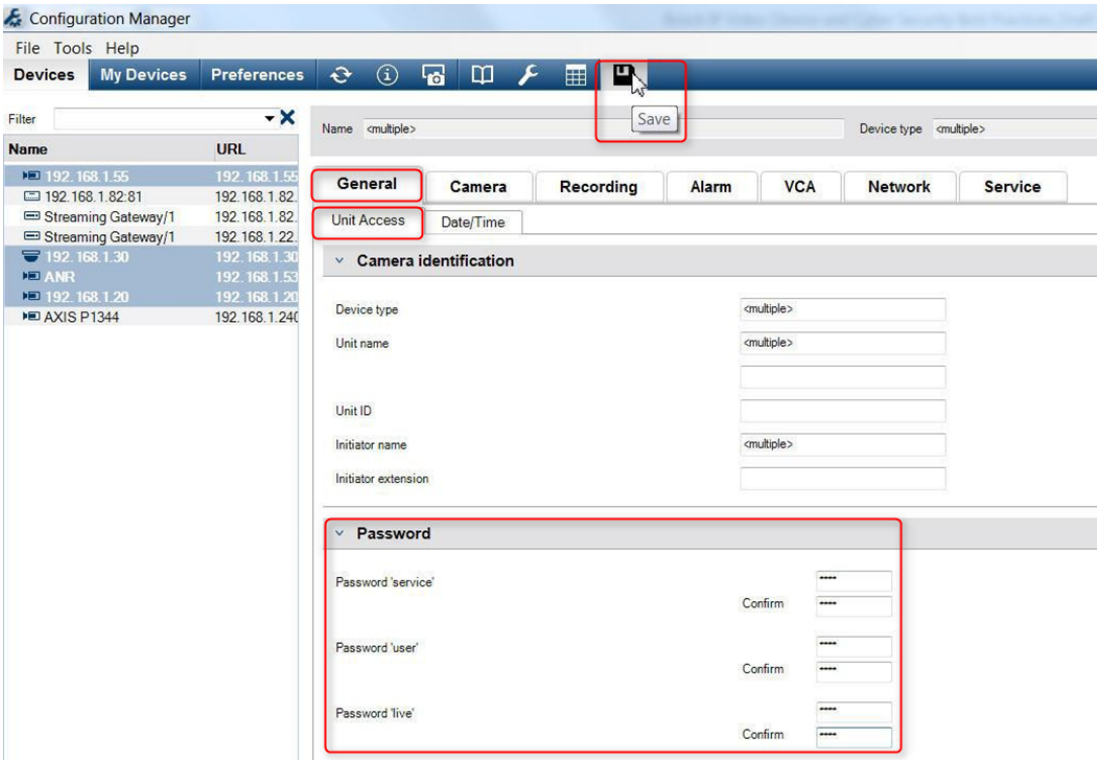
1. Чтобы добавить нового пользователя, нажмите **Добавить**.
   Отобразится всплывающее окно.
2. Введите новые данные и назначьте группу пользователя.
3. Нажмите **Установить** для сохранения изменений.

Замечание!
В версии микропрограммы 6.32 также были введены более строгие требования к паролям.
Теперь пароли должны быть как минимум 8 символов длиной.

4.2.3 Назначение паролей с помощью Configuration Manager

При использовании Bosch Configuration Manager пароли можно с легкостью задавать для отдельных или нескольких устройств одновременно.

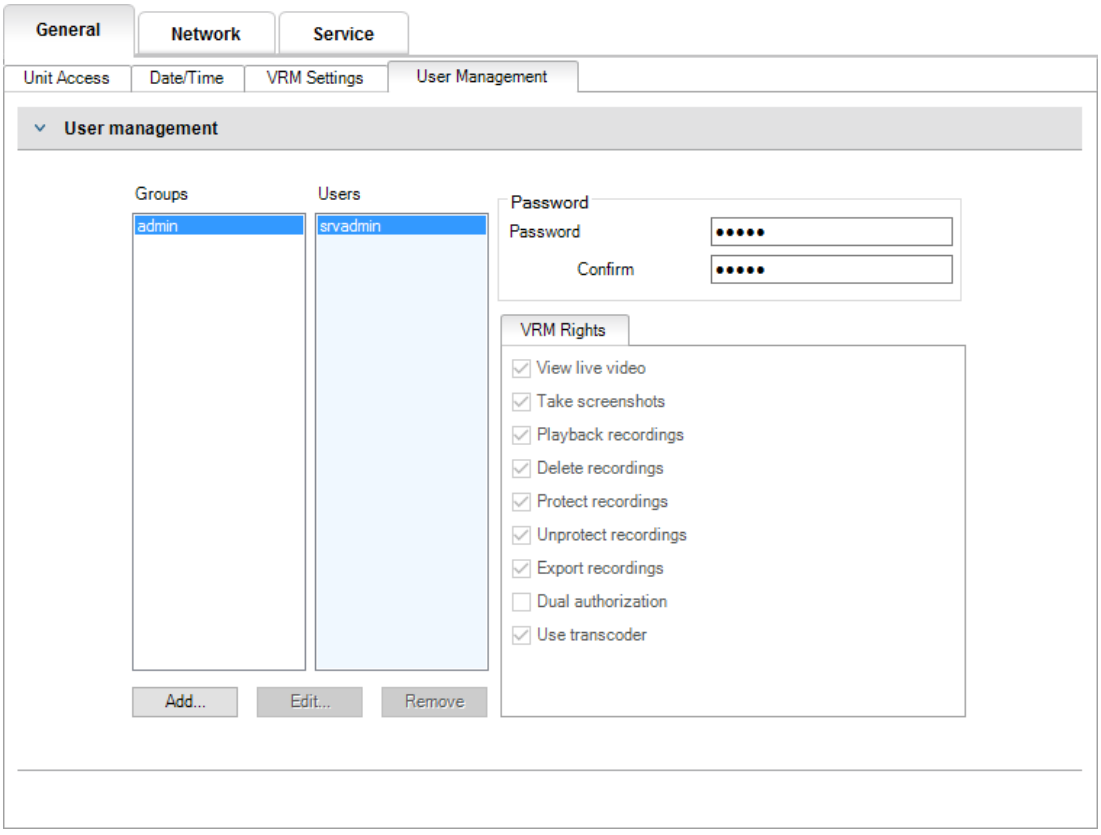
1. В Configuration Manager выберите одно или несколько устройств.
2. Выберите вкладку **Общие**, затем выберите **Доступ к устройству**.
3. В меню **Пароль** введите и подтвердите желаемый пароль для каждой из трех учетных записей (**Пароль "service"**, **Пароль "user"** и **Пароль "live"**).
4. Нажмите  для применения и сохранения изменений.



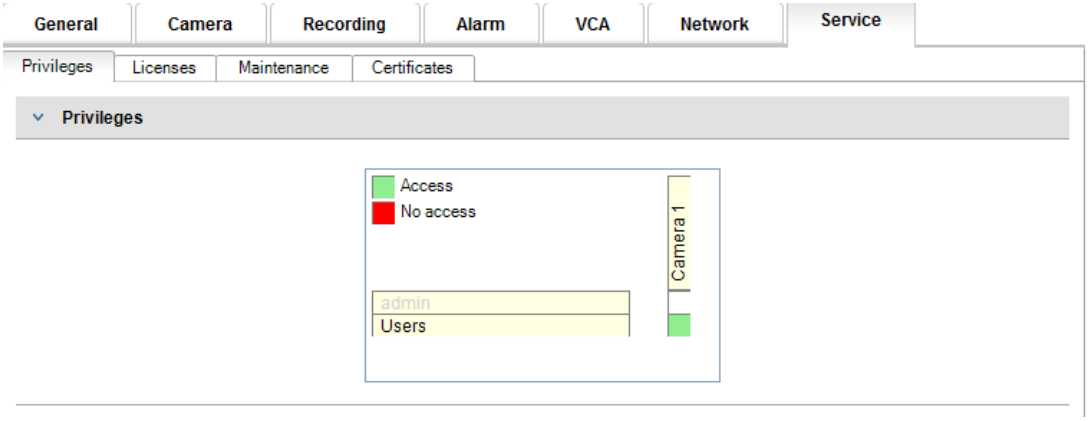
Для более крупных установок, управляемых BVMS или Video Recording Manager, установленным на записывающей устройстве, можно задать общие пароли для всех IP-видеоустройств, добавленных к системе. Это обеспечивает простоту управления и стандартный уровень безопасности по всей сети видеосистемы.

4.2.4 Назначение паролей для одиночной установки VRM

Video Recording Manager обеспечивает управление пользователями для еще большей гибкости и безопасности.
По умолчанию ни одной из учетных записей не присвоен пароль. Присвоение паролей является важнейшим этапом процесса защиты любого сетевого устройства. Настоятельно рекомендуется назначить пароли всем установленным в сети видеоустройствам.
То же относится к пользователям Video Recording Manager.



Кроме того, членам группы пользователей может быть предоставлен доступ к конкретным камерам и привилегиям. Таким образом обеспечивается подробное управление правами каждого пользователя.



4.2.5 Назначение паролей с помощью BVMS (в системе DIVAR IP или на автономных устройствах)

Защита устройств паролем

Камеры и кодеры, управляемые BVMS, могут быть защищены от несанкционированного доступа паролем.

Пароли для встроенных учетных записей пользователей кодеров / камер можно задать с помощью Configuration Client BVMS.

Для того, чтобы задать пароль для встроенных учетных записей пользователей, в Configuration Client BVMS:

1. в дереве устройств выберите желаемый кодер.
2. нажмите на кодер правой кнопкой и выберите **Изменить пароль....**
3. Введите пароль для трех встроенных учетных записей live, user и service.

Защита паролем по умолчанию

Версии BVMS 5.0 и более поздние обеспечивают возможность присвоения общих паролей на всех устройствах в видеосистемах объемом до 2000 IP-камер. Эта функция доступна в Configuration Wizard BVMS при работе с DIVAR IP 3000 или устройствами записи DIVAR IP 7000, или через Configuration Client BVMS в любой системе.

Для доступа к меню общих паролей в Configuration Client BVMS:

1. в меню **Аппаратное обеспечение** выберите **Защита устройств паролем по умолчанию...**
2. В поле **Всеобщий пароль по умолчанию** введите пароль и выберите **Принудительная защита пароля при активации**.

После сохранения и активации изменений в системе введенный пароль будет задан для учетных записей live, user и service на всех устройствах, включая учетную запись администратора в Video Recording Manager.

Замечание!

Если устройства уже имеют заданные пароли для каких-либо учетных записей, они не будут изменены.

Например, если пароль задан для учетной записи service, но не для live и user, общий пароль будет задан только для учетных записей live и user.

Конфигурация BVMS и настройки VRM

По умолчанию BVMS использует встроенную учетную запись администратора **srvadmin** для подключения к Video Recording Manager с защитой паролем. Во избежание несанкционированного доступа к Video Recording Manager учетная запись администратора **srvadmin** защищена сложным паролем.

Чтобы изменить пароль учетной записи **srvadmin**, в Configuration Client BVMS:

1. в дереве устройств выберите устройство VRM.
2. Нажмите правой кнопкой устройство VRM и выберите **Изменить пароль VRM.** Отобразится диалоговое окно **Изменить пароль...**.
3. Введите новый пароль для учетной записи **srvadmin** и нажмите **OK**.

Шифрованная связь с камерами
Начиная с версии BVMS 7.0, видеоданные в режиме реального времени и связь между камерой и Operator Client, Configuration Client, Management Server и Video Recording Manager BVMS можно зашифровать.
После активации безопасного подключения в диалоговом окне **Изменить кодер**, сервер BVMS, Operator Client и Video Recording Manager будут использовать безопасное подключение HTTPS для подключения камеры или кодера.
Внутренняя строка подключения BVMS изменится с rcpp://a.b.c.d (обычное RCP + подключение к порту 1756) на https://a.b.c.d (HTTPS-подключение к порту 443).
Для устаревших устройств, не поддерживающих HTTPS, строка подключения останется неизменной (RCP +).

Если выбрана HTTPS-связь, будет использоваться связь HTTPS (TLS) для шифрования всей полезной нагрузки управления и видео через модуль шифрования устройства. При использовании TLS все управление передачей HTTPS и полезная нагрузка видео шифруется с помощью ключа шифрования AES до 256 бит длиной.
Для активации шифрованной связи в Configuration Client BVMS:
1. в дереве устройств выберите желаемый кодер/камеру.
2. Правой кнопкой нажмите кодер/камеру и выберите **Изменить кодер**.
3. В диалоговом окне **Изменить кодер** активируйте **Подключение HTTPS.**
4. Сохраните и активируйте конфигурацию.

После активации безопасного подключения с кодером, другие протоколы можно деактивировать (см. *Общие настройки использования сетевых портов и передачи видеоданных, Страница 17*).

Замечание!
BVMS поддерживает только порт HTTPS по умолчанию 443. Использование других портов не поддерживается.

4.3 Усиление защиты доступа к устройствам

Все IP-видеоустройства Bosch поставляются со встроенными многофункциональными веб-страницами. Веб-страницы каждого конкретного устройства поддерживают как видео в режиме реального времени, так и воспроизведение записанного видеоизображения, а также предлагают ряд определенных параметров конфигурации, которые могут быть недоступны через систему управления видео. Встроенные учетные записи выступают в качестве каналов доступа к разным разделам соответствующих веб-страниц. Несмотря на то, что доступ к веб-странице невозможно отключить с помощью самой веб-страницы — для этого можно использовать Configuration Manager — существует несколько способов скрыть присутствие устройства, ограничить доступ, а также управлять использованием видеопортов.

4.3.1 Общие настройки использования сетевых портов и передачи видеоданных

Все IP-видеоустройства Bosch используют протокол дистанционного управления (RCP+) для обнаружения, управления и связи. RCP+ является запатентованным протоколом Bosch, использующим конкретные статические порты для обнаружения и связи с IP-видеоустройствами Bosch — 1756, 1757 и 1758. При работе с BVMS или другой сторонней

системой управления видео с интегрированными IP-видеоустройствами Bosch через Bosch VideoSDK перечисленные порты должны быть доступны в сети для корректной работы IP-видеоустройств.

Видеоизображение может транслироваться с устройств несколькими способами: UDP (динамический), HTTP (80) или HTTPS (443).
Использование портов HTTP и HTTPS может быть изменено (см. *HTTP, HTTPS и использование видеопортов, Страница 19*). Прежде чем вносить какие-либо изменения в порты, необходимо настроить требуемую форму связи с устройством. Меню Связь можно открыть с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Общие**, затем выберите **Доступ к устройству**.
3. Откройте часть страницы **Доступ к устройству**

4. В списке **Протокол** выберите желаемый протокол:

– RCP+
– HTTP (по умолчанию)
– HTTPS

При выборе связи через HTTPS, для связи между Configuration Manager и видеоустройствами будет использоваться HTTPS (TLS) для шифрования полезной нагрузки с помощью ключа шифрования AES до 256 битов длиной. Это бесплатная базовая функция. При использовании TLS все управление передачей и полезная нагрузка видео HTTPS шифруется через модуль шифрования устройства.

Замечание!
Шифрование предназначено специально для «тракта передачи». После получения видео программным или аппаратным декодером поток окончательно расшифровывается.

4.3.2 Минимальная версия TLS

Некоторые старые клиенты могут использовать более ранние и менее защищенные версии TLS. Однако, если это возможно, задайте минимальные требования касательно версии TLS, чтобы клиенты не переводили устройства в режим работы с менее защищенным доступом.
Выберите наиболее новую из поддерживаемых версий TLS в качестве минимального требования.

Замечание!
При определении минимального уровня безопасности для доступа к устройствам с ПО клиента убедитесь, что все порты и протоколы, допускающие более низкий уровень доступа, выключены или деактивированы на устройствах.

4.3.3 HTTP, HTTPS и использование видеопортов

Использование портов HTTP и HTTPS на всех устройствах можно изменять или отключать. Шифрованная связь может быть активирована с помощью отключения порта RCP +, а также порта HTTP, что принудительно активирует шифрование для всех видов связи. При отключенном использовании портов HTTP HTTPS останется включенным и любые попытки отключить его окончатся неудачей.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Доступ к сети**.
3. Откройте часть страницы **Подробно**.

4. В части страницы **Подробно** измените порты браузера HTTP и HTTPS, а также порт RCP+, используя раскрывающийся список:
   - изменение порта браузера HTTP: 80 или порты от 10000 до 10100
   - изменение порта браузера HTTPS: 443 или порты от 10443 до 10543
   - RCP + порт 1756: **Вкл.** или **Выкл.**

Замечание!
В микропрограмме версии 6.1, если HTTP-порт деактивирован, и совершается попытка открытия веб-страницы устройства, запрос будет направлен на заданный в данный момент HTTPS-порт.
Функция перенаправления запроса отсутствует в версиях микропрограммы 6.20 и более поздних. Если HTTP-порт деактивирован, а HTTPS-порт был настроен для использования порта, отличного от 443, доступ к веб-страницам может быть получен только с помощью перехода по IP-адресу устройства и назначенному порту.

Пример:
https://192.168.1.21:10443. Любые попытки подключения к адресу по умолчанию окончатся неудачей.

4.3.4 Видео ПО и выбор порта

Изменение этих параметров также повлияет на то, какой порт используется для передачи видео при использовании ПО для управления видео в вашей сети LAN.
Если все IP-видеоустройства настроены, например, на HTTP-порт 10000, и BVMS Operator Client настроен для «туннелирования TCP», то все передачи видеоданных в сети будут осуществляться через HTTP-порт 10000.

Замечание!
Изменения параметров портов устройств должны соответствовать параметрам системы управления и ее компонентов, а также параметрам клиентов.

Замечание!
В зависимости от сценария размещения и целей безопасности системы рекомендуемые методики могут отличаться. Отключение и перенаправление использования портов HTTP или HTTPS имеет свои преимущества. Изменение порта в любом протоколе исключает необходимость предоставления информации на средства сети, такие как NMAP (Network Mapper, бесплатный сканер безопасности). Приложения, такие как NMAP, обычно используются как средства диагностики для определения слабых мест какого-либо устройства в сети. Этот способ в сочетании с назначением надежного пароля повышает общий уровень безопасности системы.

4.3.5 Туннелирование SSH

Для удаленного доступа к устройству BVMS Operator Client по общедоступной сети система BVMS использует технологию туннелирования Secure Shell (SSH) для обеспечения безопасной (зашифрованной) связи.
Туннелирование SSH позволяет создать зашифрованный туннель с помощью подключения протокол/сокет SSH. Этот зашифрованный туннель может передавать как шифрованные, так и нешифрованные данные. Реализация Bosch SSH также использует протокол Omni-Path — высокопроизводительный протокол связи с низкой задержкой от Intel.

Подробнее о настройке службы SSH в системе BVMS см. в документации по BVMS.
Подробнее о настройке систем DIVAR IP для безопасного удаленного доступа с помощью клиента BVMS Operator Client см. в документации по DIVAR IP.

4.3.6 Доступ Telnet

Telnet — протокол на уровне приложения, который обеспечивает связь с устройствами через виртуальный терминал для обслуживания и устранения неполадок. Все IP-видеоустройства Bosch поддерживают Telnet, и поддержка Telnet по умолчанию включена в версиях микропрограммы до 6,1x. Начиная с версии микропрограммы 6.20, порт Telnet отключен по умолчанию.

Замечание!
С 2011 г. число кибератак с использованием протокола Telnet возросло. В современных условиях рекомендуется деактивация поддержки Telnet на всех устройствах до тех пор, пока протокол не потребуется для ремонта или устранения неполадок.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Доступ к сети**.
3. Откройте часть страницы **Подробно**.

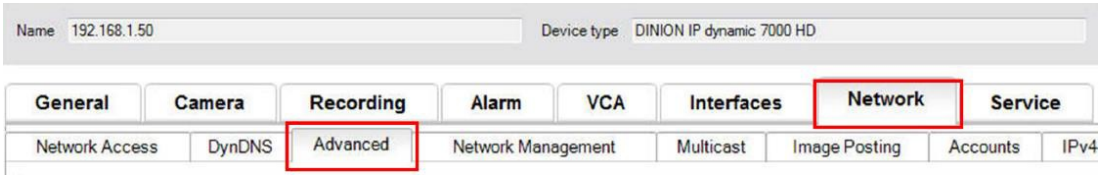
4. В части страницы **Подробно** можно **включать** или **отключать Поддержка Telnet** с использованием раскрывающегося меню.

Замечание!
Начиная с версии микропрограмм 6.20 Telnet также поддерживается с помощью так называемых «веб-разъемов», которые используют безопасные подключения HTTPS. Веб сокеты не используют стандартный порт Telnet и обеспечивают безопасный способ доступа к интерфейсу командной строки IP-устройства при необходимости.

4.3.7 Протокол RTSP: Real Time Streaming Protocol

Потоковая передача данных в реальном времени (RTSP) является основным видеокомпонентом, используемым протоколом ONVIF для обеспечения потокового видео и управления устройствами для систем управления видео, соответствующих стандартам ONVIF. RTSP также используется различными сторонними видеоприложениями для базовых функций потоковой передачи, а в некоторых случаях может использоваться для устранения неполадок устройств и сети. Все IP-видеоустройства Bosch поддерживают потоковую передачу в помощью протокола RTSP.
Функциями RTSP можно легко управлять с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Дополнительно**



3. Откройте часть страницы **RTSP**.
4. В раскрывающемся меню **Порт RTSP** отключите или измените функции RTSP:
   - порт RTSP по умолчанию: 554
   - изменение порта RTSP: от 10554 до 10664

Замечание!
В последнее время появляется все больше сообщений о кибератаках с использованием буферных атак с помощью переполнения стека RTSP. Эти атаки были нацелены на устройства конкретных поставщиков. Рекомендуемой методикой является отключение этого сервиса, если он не используется системой управления видео, соответствующей стандартам ONVIF, или для базовой потоковой передачи в режиме реального времени. Кроме того, если это позволяет принимающий клиент, связь RTSP может быть туннелирована с использованием подключения HTTPS, которое на данный момент является единственным способом передачи шифрованных данных RTSP.

Замечание!
Подробнее о RTSP см. в примечании по применению *Использование RTSP с устройствами Bosch VIP* в электронном каталоге продуктов Bosch Security Systems по следующей ссылке:
https://resources-boschsecurity-cdn.azureedge.net/public/documents/RTSP_VIP_Application_note_enUS_9007200806939915.pdf

4.3.8 UPnP: функция Universal Plug and Play

IP-видеоустройства Bosch способны обеспечивать связь с устройствами сети с помощью функции **UPnP**. Эта функция в основном используется в малых системах с небольшим количеством камер, в которых камеры автоматически отображаются в каталоге сети ПК и могут быть с легкостью найдены. Но они также отображаются и для любого другого устройства в сети.

UPnP можно отключить с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Управление сетью**

3. Откройте часть страницы **UPnP**.
4. В раскрывающемся меню **UPnP** выберите **Отключить** для отключения **UPnP**.

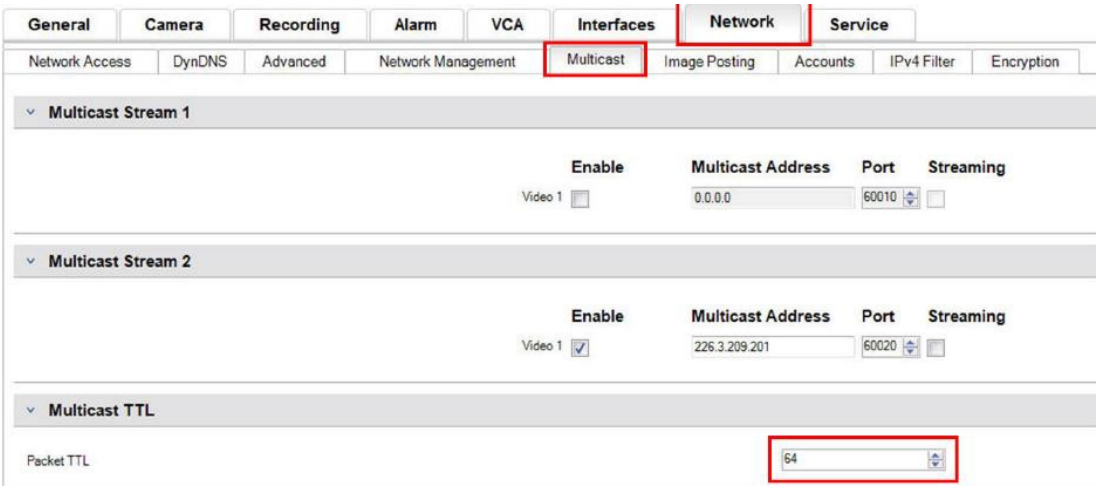
Замечание!
UPnP не следует использовать в крупных установках в связи с большим числом уведомлений о регистрации и потенциальным риском нежелательного доступа или атаки.

4.3.9 Многоадресная передача

Все IP-видеоустройства Bosch способны обеспечивать как «Многоадресную передачу видео по запросу», так и «Многоадресную потоковую передачу видео». Если одноадресная передача видео основывается на адресате данных, многоадресная основывается на источнике, что может привести к возникновению проблем безопасности на уровне сети, таких как: управление групповым доступом, надежность центра группы и надежность роутера. При том, что конфигурация роутера не рассматривается в данном руководстве, существует решение в области безопасности, которое можно внедрить с самого IP-видеоустройства.

Правило TTL (time-to-live, время жизни) определяет, куда и как далеко многоадресный поток данных может перемещаться внутри сети, каждый переход при этом уменьшает его «время жизни» на одну единицу. При настройке IP-видеоустройства для многоадресного использования можно изменить TTL-пакет устройства.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Многоадресная передача**
3. Откройте часть страницы **TTL при многоадресной передаче**.
4. Измените настройки **TTL пакета** с использованием следующих значений TTL и ограничений областей:
   - значение TTL 0 = ограничено доступом к локальному узлу
   - значение TTL 1 = ограничено доступом к той же подсети
   - значение TTL 15 = ограничено доступом к тому же объекту
   - значение TTL 64 (по умолчанию) = ограничено доступом к той же области
   - значение TTL 127 = по всему миру
   - значение TTL 191 = по всему миру с ограниченной полосой пропускания
   - значение TTL 255 = неограниченные данные

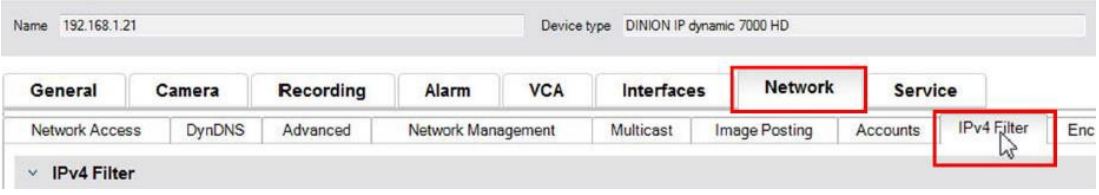


Замечание!
При работе с данными видеонаблюдения рекомендуется установить значение TLL равным 15, ограничив их перемещение тем же объектом. Если вы знаете точное максимальное число переходов, рекомендуется использовать его в качестве значения TTL.

4.3.10 Фильтр IPv4

Вы можете ограничить доступ к любому IP-видеоустройству Bosch с помощью функции фильтра IPv4. Фильтр IPv4 использует базовые функции создания подсети для задания до двух допустимых диапазонов IP-адресов. Как только диапазоны заданы, фильтр ограничивает доступ с любых IP-адресов, не входящих в данные диапазоны.

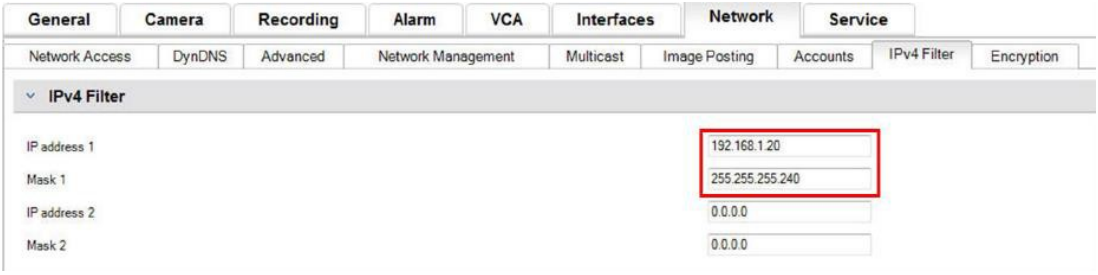
1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **IPv4-фильтр**.



Замечание!
Для успешной настройки данной функции необходимо иметь базовое представление о формировании подсетей или иметь доступ к калькулятору подсетей. Ввод неверных значений для данных параметров может ограничить доступ к самому устройству, и для восстановления доступа потребуется сброс до заводских настроек.

3. Для создания правила фильтра введите два значения:
   - Введите базовый IP-адрес, соответствующий правилу подсети, которое вы создаете.
     Базовый IP-адрес указывает, какую подсеть вы допускаете, и обязательно должен входить в желаемый диапазон.
   - Введите маску подсети, которая определяет IP-адреса, с которыми IP-видеоустройства будут поддерживать связь.

В следующем примере **IP-адрес 1** был введен как 192.168.1.20, а **Маска 1** как 255.255.255.240. Такие параметры ограничат доступ со всех устройств, попадающих в заданный IP-диапазон от 92.168.1.16 до 192.168.1.31.



При использовании функции**IPv4-фильтр** устройства могут сканироваться с помощью RCP +, но доступ к параметрам конфигурации и видео невозможен через клиентов, которые находятся вне диапазона разрешенных IP-адресов. Это включает доступ через веб-браузер.
Само IP-видеоустройство не обязательно должно быть расположено в допустимом диапазоне адресов.

Замечание!
В зависимости от особенностей вашей системы использование функции **IPv4-фильтр** может снизить нежелательную видимость устройств в сети. При активации этой функции обязательно задокументируйте параметры для последующего использования.
Обратите внимание, что доступ к устройству все еще можно будет получить с помощью IPv6, поэтому использование фильтра IPv4 имеет смысл только в сетях, использующих исключительно IPv4.

4.3.11 SNMP

Протокол SNMP (Simple Network Management Protocol, протокол простого управления сетями) — это распространенный протокол для мониторинга рабочего состояния системы. Такая система наблюдения обычно имеет сервер централизованного управления, который собирает все данные совместимых компонентов и устройств системы.
SNMP обеспечивает два способа получения сведений о состоянии системы:

- Сервер управления сетью может запрашивать данные о состоянии устройства с помощью SNMP-запросов.
- Устройства могут активно сообщать серверу управления сетью о своем состоянии системы в случае ошибки или тревожных событий с помощью отправки SNMP-запросов на SNMP-сервер. Такие запросы должны быть настроены внутри устройства.

SNMP также позволяет настраивать некоторые переменные внутри устройств и компонентов.
Сведения, тип сообщений, поддерживаемый устройством, и тип запросов, которые оно может отправлять, содержатся в базе информации управления (Management Information Base), так называемом файле MIB — файле, поставляемом в комплекте с продуктом в целях простоты интеграции в систему сетевого мониторинга.

Существует три различные версии протокола SNMP:

- SNMP версии 1
  SNMP версии 1 (SNMPv1) – это первоначальное применение протокола SNMP. Он широко используется и стал фактически стандартным протоколом для контроля и управления сетями.
  Но SNMPv1 оказался под угрозой в связи с отсутствием функций безопасности. Он использует только "*строки сообщества*"в качестве паролей, которые передаются

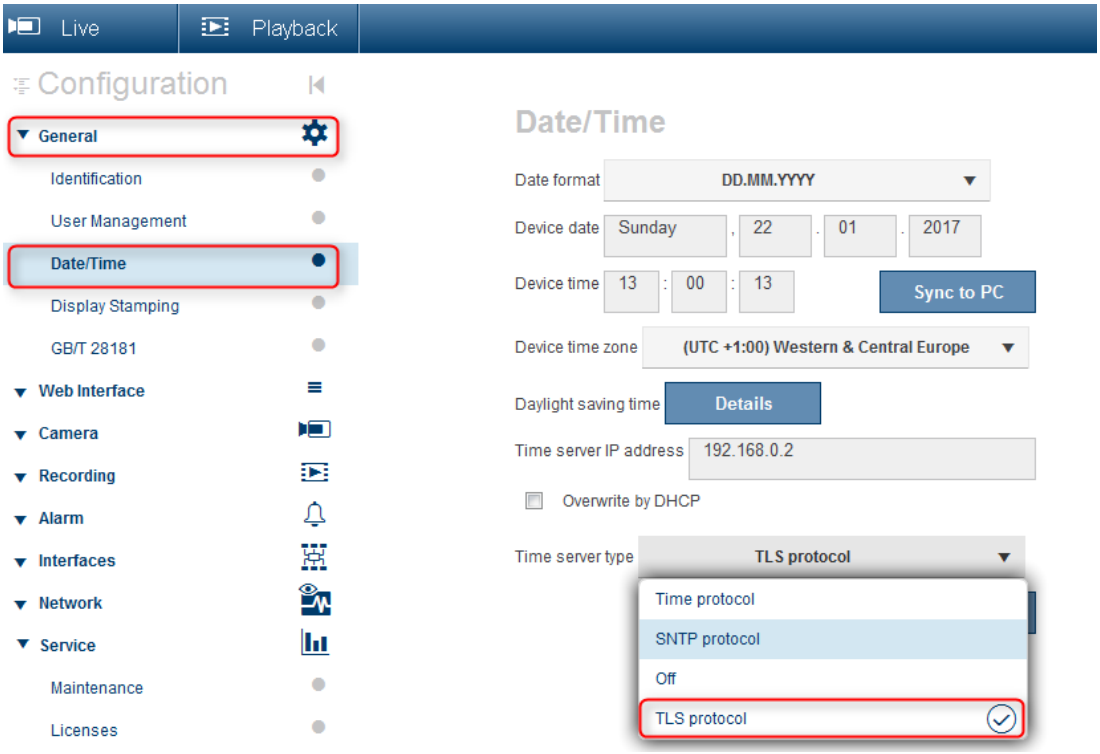
открытым текстом.
Таким образом, SNMPv1 следует использовать только тогда, когда есть гарантия, что сеть физически защищена от несанкционированного доступа.

– SNMP версии 2
  SNMP версии 2 (SNMPv2), помимо прочего, включает ряд улучшений в области безопасности и конфиденциальности, а также возможность создания массового запроса для извлечения большого объема данных по одному запросу. Однако, его концепция безопасности считается слишком сложной, что и воспрепятствовало его принятию.
  Таким образом, он был вскоре вытеснен версией SNMPv2c, соответствующей версии SNMPv2, но без противоречивой модели безопасности. Эта версия возвращается к методу, основанному на сообществе, используемому в SNMPv1, и имеет аналогичные пробелы в безопасности.
– SNMP версии 3
  В SNMP версии 3 (SNMPv3) в основном добавлены функции безопасности и улучшения удаленной конфигурации. Они включают в себя улучшения конфиденциальности с использованием шифрования пакетов, целостности сообщений и проверки подлинности.
  Эта версия также решает проблему крупномасштабного применения SNMP.

Замечание!
Как SNMPv1, так и SNMPv2c оказались под угрозой в связи с отсутствием в них функций обеспечения безопасности. Они используют только «строки сообщества» в качестве паролей, которые передаются в виде открытого текста.
Таким образом, SNMPv1 или SNMPv2c следует использовать только тогда, когда есть гарантия, что сеть физически защищена от несанкционированного доступа.
На сегодняшний день камеры Bosch поддерживают только SNMPv1. Убедитесь, что SNMP отключен, если вы его не используете.

4.3.12 Защищенная временная основа

В дополнение к протоколу времени и протоколу SNTP (оба протокола являются незащищенными), в версии микропрограммы 6.20 был введен третий режим клиента сервера времени, использующий протокол TLS. Этот метод также широко известен как *TLS-Date*.
В этом режиме любой произвольный сервер HTTPS можно использовать как сервер времени. Значение времени определяется как побочный эффект процесса квитирования HTTPS. Передача данных защищена TLS. Дополнительный корневой сертификат для сервера HTTPS можно загрузить в хранилище сертификатов камеры для проверки подлинности сервера.



Замечание!
Убедитесь, что введенный IP-адрес сервера времени имеет стабильную и надежную временную базу.

4.3.13 Облачные сервисы

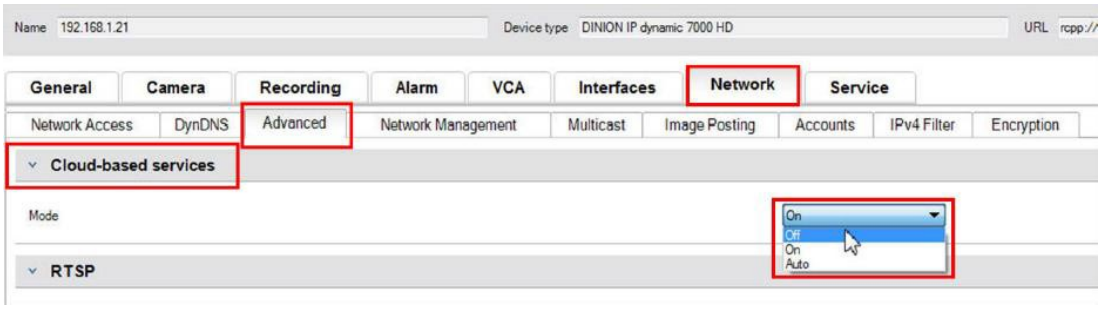
Все IP-видеоустройства Bosch могут связываться с облачными сервисами Bosch, такими как Remote Portal. В зависимости от региона размещения это позволяет IP-видеоустройствам Bosch использовать такие сервисы, как Remote Device Management или Cloud VMS, а также направлять сигналы тревоги и другие данные на центральную станцию. Подробнее см. в базе знаний Bosch Building Technologies: https://community.boschsecurity.com.

Существует три режима использования облачных сервисов:

– **Вкл.**:
  видеоустройство постоянно подключено к облачному серверу.
– **Авто** (по умолчанию):
  видеоустройства будут пытаться связываться с сервером несколько раз, в случае неудачи попытки связаться с облачным сервером будут прекращены.
– **Выкл.**
  отправка запросов на облачный сервер не выполняется.

Облачные сервисы можно легко отключить с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, а затем выберите вкладку **Дополнительно**.
3. Найдите раздел страницы **Облачные сервисы** и выберите из списка **Выкл**.



Замечание!
Если вы используете облачные сервисы Bosch, оставьте конфигурацию по умолчанию. Во всех других случаях установите режим облачных сервисов **Выкл.**

4.4 Усиление безопасности IP-камер

IP-камеры Bosch поставляются с конфигурацией по умолчанию, которая обеспечивает простую интеграцию в различные среды.
В зависимости от целевой среды и требуемого уровня ее безопасности может понадобиться изменить отдельные настройки камеры, чтобы повысить кибербезопасность и защищенность данных.
Однако могут существовать ограничения операционной среды, обязывающие использовать определенные менее безопасные протоколы или функции (например, SNMPv1).

4.4.1 Уровни усиления безопасности

Существует два уровня усиления безопасности: *повышенный* и *строгий*.
Строгий уровень усиления безопасности устанавливает наиболее безопасные настройки, но может ограничивать использование некоторых возможностей устройства, поскольку такие функции, как автоматическое обнаружение устройства, отключены. Следует оценивать отдельно для каждой функции, можно ли применить *повышенные* или *строгие* настройки усиления безопасности.

4.4.2 Обзор уровня усиления безопасности

Сеть - Сетевые службы	**По умолчанию**	**Повышенный**	**Строгий**
HTTP	Активирован	Отключен	Отключен
HTTPS	Активирован	Активирован	Активирован
RTSP	Активирован	Дополнительно	Отключен
RCP	Активирован	Отключен	Отключен
SNMPv1	Отключен	Отключен	Отключен
SNMPv3	Отключен	Активирован	Активирован
iSCSI	Активирован	Дополнительно	Отключен
UPnP	Отключен	Отключен	Отключен
Сервер NTP	Отключен	Отключен	Отключен
Discovery	Активирован	Активирован	Отключен

Сеть - Сетевые службы	По умолчанию	Повышенный	Строгий
ONVIF Discovery	Активирован	Активирован	Отключен
GBT/28181	Отключен	Отключен	Отключен
Механизм сброса пароля	Активирован	Отключен	Отключен
Отклик ping	Активирован	Активирован	Отключен
RTSPS	Активирован	Активирован	Активирован
HTTP	Активирован	Отключен	Отключен

Сеть - Доступ к сети	По умолчанию	Повышенный	Строгий
Минимальная версия TLS	1.0	1.2	1.2
HSTS	Отключен	Активирован	Активирован

Сеть - Дополнительно	По умолчанию	Повышенный	Строгий
802.1x	Отключен	Дополнительно	Активирован
Syslog	Отключен	TCP	TLS

Сеть - Управление сетью	По умолчанию	Повышенный	Строгий
Режим SNMPv3	Отключен	SHA1 / AES	SHA1 / AES

Сеть - IPv4-фильтр	По умолчанию	Повышенный	Строгий
Фильтр IPv4	Отключен	Активирован	Активирован

Общие - Дата/Время	По умолчанию	Повышенный	Строгий
Дата/время (клиент NTP)	Отключен	Дата SNTP / TLS	Дата TLS

Подключение - Облачные службы	По умолчанию	Повышенный	Строгий
Remote Portal	Отключен	Активирован	Активирован

Обслуживание - Журнал	По умолчанию	Повышенный	Строгий
Защита ПО	Отключен	Активирован	Активирован

4.4.3 Описание функций и рекомендации по усилению безопасности

HTTP

По умолчанию используется протокол HTTP без шифрования, поэтому учетные данные или настройки, если они используются, передаются в незашифрованном виде.
Рекомендация. Необходимо отключить обычный протокол HTTP и включить зашифрованный HTTPS, особенно при подключении к ненадежной сети.

HTTPS

В протоколе HTTPS применяется шифрование, поэтому он должен по умолчанию использоваться для доступа к веб-интерфейсу или веб-API RCP. Рекомендуется использовать собственные PKI и сертификаты.
Рекомендация. HTTPS является безопасным протоколом по умолчанию для конфигурации и должен оставаться включенным.

RTSP

RTSP используется для потоковой передачи видео, но обычно он не поддерживает шифрование. Если программное обеспечение, принимающее видеопоток, поддерживает протокол RTSPS, то обычный RTSP рекомендуется отключить. При использовании других компонентов Bosch (например, декодеров/BVMS/VRM/DIVAR IP) можно включить запатентованное шифрование Bosch для протокола RTSP, которое обеспечивает безопасную передачу данных.
Рекомендация. Если видеоданные могут передаваться в незашифрованном виде или с шифрованием от Bosch, стоит использовать риск-ориентированный подход. По возможности используйте зашифрованный протокол RTSPS

RCP

Запатентованный расширенный протокол дистанционного управления Bosch (RCP+) — это протокол конфигурации для IP-камер Bosch. Обычный RCP не поддерживает шифрование, поэтому настройки передаются незашифрованными. Все инструменты Bosch на сегодняшний день используют связь по протоколу RCP вместо HTTPS, однако более старый протокол может потребоваться для некоторых сторонних инструментов интеграции или средств создания сценариев, все еще полагающихся на него.
Рекомендация. Отключите протокол RCP, если он не используется сторонними инструментами или устаревшими системами.

SNMPv1

SNMP — это распространенный протокол сетевого мониторинга, используемый для запроса информации о состоянии устройства или отправки ловушки удаленному получателю, однако этот протокол не использует шифрование.
Рекомендация. Не включайте протокол, если он не требуется для мониторинга состояния или обеспечения совместимости. По возможности используйте SNMPv3.

SNMPv3

Протокол SNMPv3 является развитием SNMPv1 и может использовать шифрование.

Рекомендация. Рекомендуется к применению, если необходимо использовать мониторинг SNMP.

iSCSI
Отключает внутренний сервер iSCSI, который используется для того, чтобы внутренние записи камеры были доступны посредством iSCSI. iSCSI — это протокол, не поддерживающий шифрование.
Рекомендация. Отключите сервер iSCSI, если он не используется в камере.

UPnP
Обнаружение камеры с помощью протокола UPnP.
Рекомендация. Отключите архитектуру UPnP, если она не требуется.

Сервер NTP
Включите сервер NTP на камере, чтобы другие устройства или камеры могли синхронизировать с ней время. Если это возможно, выделенное устройство должно передавать данные времени в сеть камер, обеспечивая разделение функций. Если же другое устройство отсутствует, данные времени могут передаваться камерой.
Рекомендация. Сервер NTP должен быть отключен, если в нем нет необходимости.

Discovery
Использование запатентованного механизма Bosch для обнаружения камер с помощью программного обеспечения Bosch, такого как Configuration Manager.
Рекомендация. При работе с динамическими IP-адресами эта функция должна оставаться включенной. При работе в среде с фиксированными IP-адресами ее можно отключить.

ONVIF Discovery
Поддержка обнаружения камер посредством протокола ONVIF Discovery
Рекомендация. При работе с динамическими IP-адресами и инструментами, совместимыми с ONVIF, эта функция должна оставаться включенной. При работе в фиксированной среде с фиксированными IP-адресами ее можно отключить.

GBT/28181
GBT/28181 — это китайский стандарт обеспечения функциональной совместимости между различными устройствами.
Рекомендация. Не включайте, если он не требуется.

Механизм сброса пароля
IP-камеры могут устанавливаться в очень удаленных местах, что затрудняет техническое обслуживание или сброс настроек до заводских в случае блокировки доступа к камере. Компания Bosch предлагает возможность сброса пароля камеры с помощью механизма запроса и ответа на основе защищенного механизма открытых и закрытых ключей.
Рекомендация. Рекомендуется выключить эту функцию, если она не требуется.

Отклик ping
Определяет, отвечает ли камера на запросы ping в сети. Может помочь при отладке. В высокозащищенной сети эту функцию можно отключить, чтобы устранить возможность перечисления устройств с помощью эхо-тестирования адресов, хотя существует несколько других способов обнаружения устройств, которые могут быть использованы злоумышленниками.
Рекомендация. Риск-ориентированный подход; может быть отключен для высокозащищенных сетей.

RTSPS
RTSPS — это версия протокола RTSP с поддержкой шифрования, использующаяся для потоковой передачи видео. Если принимающее программное обеспечение поддерживает протокол RTSPS, его следует всегда использовать вместо обычного RTSP. Поскольку многие клиенты RTSP не поддерживают защищенный вариант, на уровне безопасности 1 остается включенным протокол RTSP.
Рекомендация. По возможности используйте RTSPS.

Минимальная версия TLS
IP-камеры не допускают использования незащищенного протокола SSLv3 или более старых протоколов подключения. Версии протокола TLS 1.0 и 1.1 признаны IETF устаревшими и имеют известные уязвимости (BEAST, FREAK).
Камеры CPP4, CPP6, CPP7 и CPP7.3 поддерживают безопасную версию TLS 1.2, которая должна быть установлена как минимально необходимая.
Камеры CPP13 и CPP14 не поддерживают версии TLS старее 1.2. Они также поддерживают более новые спецификации TLS 1.3.
Рекомендация. Установите версию TLS 1.2 в качестве минимально необходимой.

HSTS
HTTP Strict Transport Security (HSTS) — это политика, устанавливаемая веб-сайтом для защиты от атак посредника и атак путем понижения версии протокола. Она позволяет веб-сайту обязать браузер использовать только соединения по протоколу HTTPS в рамках данного подключения, не используя никаких соединений HTTP без шифрования.
Рекомендация. Включите HSTS на камере.

802.1x
802.1x — это стандарт управления доступом к сети (NAC). Он позволяет проверить подлинность устройств в сети и предоставить доступ к сети только тем устройствам, подлинность которых подтверждена. IP-камеры Bosch поддерживают стандарт 802.1x с проверкой подлинности с помощью пароля или сертификата. Предпочтительным методом является проверка подлинности с помощью сертификата. Для использования стандарта 802.1x необходим сетевой коммутатор, который его поддерживает, а также сервер проверки подлинности.
Рекомендация. Если инфраструктура сети позволяет это, используйте проверку подлинности в сети по стандарту 802.1x.

Syslog
Поскольку камера предоставляет лишь ограниченное пространство для хранения сообщений журнала, эти сообщения должны отправляться в центральный пункт и анализироваться там для выявления атак и неправильных конфигураций.
Рекомендация. Используйте TCP Syslog для предотвращения утраты сообщений из-за потери пакетов. Используйте Syslog с TLS для шифрования и проверки подлинности сообщений.

Режим SNMPv3
SNMPv3 является развитием протокола SNMPv1 и обеспечивает безопасную проверку подлинности и передачу информации.
Рекомендация. При использовании протокола SNMPv3 используйте SHA1 как протокол проверки подлинности и AES как протокол конфиденциальности (если поддерживается).

IP-фильтр
В IP-фильтре можно определить несколько IP-адресов (отдельных хостов или подсетей сети), которым разрешен доступ к камере. Рекомендуется указать в нем компьютеры или сети, имеющие доступ к камере.
Рекомендация. Рекомендуется использовать IP-фильтр для определения разрешенных хостов или сетей.

Дата/Время
Чтобы в журналах и видеоданных была указана правильная метка времени, рекомендуется синхронизировать время с центральным сервером времени. Для этого можно использовать дату SNTP и TLS. Преимуществом SNTP является более точная синхронизация времени. Преимуществом TLS является возможность проверки правильности сертификата, что делает этот протокол более надежным решением.
Рекомендация. Используйте безопасные средства синхронизации времени с датой SNTP или TLS.

Облачные сервисы
Компания Bosch предлагает свои облачные сервисы для управления камерами в облаке Bosch (Remote Portal). Облачные сервисы не подключаются к порталу Remote Portal автоматически и по умолчанию отключены. Если необходимо использовать Remote Portal, каждую камеру сперва нужно подключить к нему отдельно. Для обеспечения безопасного соединения между Remote Portal и камерой предприняты все меры предосторожности, поэтому при необходимости Remote Portal можно использовать в любой среде.
Рекомендация. Remote Portal можно использовать в зависимости от того, используется ли облачное решение.

Защита ПО
После завершения конфигурации IP-камеры параметры устройства не должны изменяться. Для оповещения об изменении конфигурации устройства можно включить защиту программного обеспечения.
Рекомендация. Если изменений в конфигурации не ожидается, включите функцию защиты программного обеспечения.

4.4.4 Углубленная защита

Углубленная защита — это многоуровневый подход к безопасности, подразумевающий, что для обеспечения безопасности продукта применяются не отдельные меры, а несколько слоев защиты, и для получения несанкционированного доступа к продукту злоумышленнику необходимо взломать каждый из них. Кроме того, при выпуске каждой версии продукта проводится оценка необходимости новых функций для предотвращения новых типов атак и повышения общей защищенности продукта.
Ниже приведен обзор основных функций обеспечения безопасности IP-камеры.

- **Подписывание микропрограммы**
  Каждый файл обновления микропрограммы зашифрован и подписан сертификатом Bosch. На камеры могут быть установлены только обновления, опубликованные компанией Bosch, что предотвращает установку вредоносных микропрограмм.
- **Безопасная загрузка**
  Камеры платформ CPP13, CPP14 и более новых оснащены механизмом безопасной загрузки. Безопасная загрузка проверяет целостность всей системы, начиная с загрузчика и заканчивая микропрограммой камер. Каждый шаг процесса загрузки проверяет следующий, начиная с неизменяемого аппаратного корня доверия. Это не позволяет злоумышленнику внести изменения в загрузчик или микропрограмму устройства.
- **Брандмауэр для входа в систему**
  Чтобы защитить от атак методом перебора паролей и DoS-атак, а также обеспечить администраторам возможность входить в систему, брандмауэр для входа в систему проверяет попытки входа путем анализа поведения и в динамическом режиме блокирует или предоставляет доступ на основе IP-адресов.
- **Проверка подлинности камер**
  Для идентификации и проверки подлинности камер при производстве каждой камеры создается уникальный сертификат устройства Bosch. Этот сертификат можно использовать, чтобы проверить, действительно ли подключение выполняется к подлинному устройству Bosch. Кроме того, имеется возможность создать на камере или загрузить на нее настраиваемые сертификаты для обеспечения интеграции со средой PKI с целью защиты от атак посредника.

4.5 Повышение уровня безопасности хранилищ

Так как IP-камеры и кодеры Bosch способны устанавливать сеанс iSCSI напрямую с диском iSCSI и записывать видеоданные на диск iSCSI, устройства iSCSI должны быть подключены к той же сети LAN или WAN, что и периферийные устройства Bosch.
Для предотвращения несанкционированного доступа к записанным видеоданным устройства iSCSI должны быть защищены от несанкционированного доступа:

- Используйте проверку подлинности с помощью пароля через CHAP для обеспечения доступа к целевому устройству iSCSI только для известных устройств. Задайте пароль CHAP на целевом устройстве iSCSI и введите настроенный пароль в конфигурацию VRM. Пароль CHAP действителен для VRM и автоматически отправляется на все устройства. Если пароль CHAP используется в среде VRM BVMS, все системы хранения должны использовать тот же пароль.
- Удалите все имена пользователей и пароли по умолчанию с целевого устройства iSCSI.
- Используйте надежный пароль для учетной записи администратора целевого устройства iSCSI.

– Отключите доступ администратора через Telnet для целевых устройств iSCSI. Вместо этого используйте доступ через SSH.
– Защитите консольный доступ к целевому устройству iSCSI с помощью надежного пароля.
– Отключите неиспользуемые карты сетевого интерфейса.
– Контролируйте состояние системы хранилищ iSCSI с помощью сторонних инструментов для выявления ошибок.

4.5.1 Установка пароля CHAP на устройствах iSCSI

При установке глобального пароля CHAP в BVMS Configuration Client он автоматически передается на все кодеры, декодеры и устройства VSG.
Некоторые устройства iSCSI не поддерживают эту функцию. На таких устройствах пароль CHAP нужно установить вручную.

Замечание!
Перед добавлением устройств iSCSI в систему BVMS необходимо установить на них глобальный пароль CHAP.
Устройства iSCSI невозможно добавить в конфигурацию BVMS, в которой уже активирован глобальный пароль CHAP.

Ручная установка пароля CHAP на устройстве iSCSI (например, на DIVAR IP), работающем на последней версии операционной системы Microsoft Windows Server:

1. Откройте **Диспетчер сервера** и перейдите в меню **Файловые службы и службы хранилища > iSCSI.**
2. В списке **ЦЕЛЕВЫЕ ОБЪЕКТЫ ISCSI** щелкните нужный целевой объект iSCSI правой кнопкой мыши и нажмите **Свойства**.
   Отобразится диалоговое окно **Свойства**.
3. В диалоговом окне **Свойства** нажмите **Безопасность** и установите флажок **Включить CHAP**.
4. Введите следующие значения:
   – **Имя пользователя:** user
   – **Пароль:** введите глобальный пароль CHAP, заданный в BVMS Configuration Client (в меню **Оборудование > Защитить хранилища iSCSI паролем CHAP....**).
5. Нажмите **ОК**.
   Пароль CHAP назначен целевому объекту iSCSI.

4.6 Усиление безопасности серверов

4.6.1 Рекомендуемые настройки оборудования для серверов

– BIOS сервера позволяет устанавливать пароли более низкого уровня.
  Эти пароли запрещают определенным лицам запускать компьютер, запускать подключаемые устройства, а также изменять параметры BIOS или интерфейса UEFI (единый расширяемый микропрограммный интерфейс) без разрешения.
– Во избежание передачи данных серверу, порты USB и CD / DVD-привод должны быть отключены.
  Также необходимо отключить неиспользуемые порты NIC и такие порты управления, как интерфейс HP ILO (HP Integrated Lights-Out); консольные порты должны быть отключены или защищены паролями.

4.6.2 Рекомендуемые настройки безопасности для операционной системы Windows

Серверы должен быть частью домена Windows.
При интеграции серверов в домен Windows пользователи сети получают разрешение на доступ через центральный сервер. Так как эти учетные записи часто имеют требования к надежности и сроку действия пароля, такая интеграция может повысить уровень безопасности по сравнению с местными учетными записями, которые не имеют таких ограничений.

4.6.3 Обновления для Windows

Обновления программного обеспечения Windows следует регулярно устанавливать и отслеживать. Обновления Windows часто включают в себя исправления для недавно обнаруженных пробелов в безопасности, таких как уязвимость Heartbleed SSL, затронувшая миллионы компьютеров по всему миру. Исправления для таких значительных проблем следует устанавливать.

4.6.4 Установка антивирусного ПО

Установите антивирусное и антишпионское ПО и обеспечьте его регулярное обновление.

4.6.5 Рекомендуемые настройки для операционной системы Windows

Следующие параметры локальной групповой политики — это рекомендуемые групповые параметры в серверной операционной системе Windows. Чтобы изменить политики локального компьютера (LCP) по умолчанию, используйте редактор локальной групповой политики (LGP).
Вы можете открыть редактор LGP с помощью командной строки или используя консоль управления Microsoft (MMC).

Чтобы открыть редактор LGP из командной строки:

- нажмите **Пуск**, в поле поиска **Пуск** введите **gpedit.msc** и нажмите Enter.

Чтобы открыть редактор LGP как встраиваемый модуль MMC:

1. нажмите **Пуск**, в поле поиска **Пуск** введите **mmc** и нажмите клавишу Enter.
2. В диалоговом окне **добавления и удаления встраиваемых модулей** нажмите **редактор объектов групповой политики** и нажмите кнопку **добавить**.
3. В диалоговом окне **выберите объект групповой политики** нажмите **обзор**.
4. Нажмите **компьютер** для изменения объекта локальной групповой политики и нажмите кнопку **пользователи** для изменения объектов групповой политики администратора, не администратора и пользователя.
5. Нажмите **Готово**

4.6.6 Активировать контроль учетных записей на сервере

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Локальная политика -> Настройки безопасности

Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора	Активирован
Контроль учетных записей: позволить приложениям UIAccess запрашивать расширение прав доступа без использования безопасного рабочего стола	Отключен

Контроль учетных записей: запрос на расширение прав администратором в режиме одобрения администратором	Запрос разрешения
Контроль учетных записей: запрос на расширение прав для обычных пользователей	Запрос учетных данных в системе безопасного рабочего стола
Контроль учетных записей: обнаружение установки приложений и запрос расширения прав	Активирован
Контроль учетных записей: расширять права только для подписанных и проверенных исполняемых файлов	Отключен
Контроль учетных записей: все администраторы работают в режиме одобрения администратором	Активирован
Контроль учетных записей: переключение в режим безопасного рабочего стола при выполнении запроса на расширение прав	Активирован
Контроль учетных записей: виртуализация ошибок записи в файл и реестр в пользовательское расположение	Активирован

Политики локального компьютера -> Конфигурация компьютера -> Шаблоны администратора -> Компоненты Windows -> Интерфейс учетных данных пользователя

Нумеровать учетные записи администратора при расширении прав	Отключен

4.6.7 Отключение автозапуска

Политики локального компьютера -> Конфигурация компьютера -> Шаблоны администратора -> Компоненты Windows -> Политика автозапуска

Отключить автозапуск	Включить все диски
По умолчанию для автозапуска	Флажок установлен, не выполнять команды автозапуска
Отключить автозапуск для недисковых устройств	Активирован

4.6.8 Внешние устройства

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Локальная политика -> Настройки безопасности

Устройства: разрешить отстыковку без выполнения входа	Отключен
Устройства: разрешено форматирование и извлечение подключаемых устройств	Администраторы
Устройства: не позволять пользователям устанавливать драйверы принтера	Активирован
Устройства: предоставлять доступ к CD-ROM только пользователям, выполнившим вход на местном уровне	Активирован

Устройства: предоставлять доступ к дискетному приводу только пользователям, выполнившим вход на местном уровне	Активирован

4.6.9 Конфигурация назначения прав пользователя

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Назначение прав пользователя

Доступ к диспетчеру учетных данных в качестве надежного оператора	Никто
Доступ к компьютеру через сеть	Проверенные пользователи
Действовать как часть операционной системы	Никто
Добавить рабочие станции к домену	Никто
Разрешить вход через службы удаленного рабочего стола	Администраторы, пользователи удаленного рабочего стола
Изменить время системы	Администраторы
Изменить часовой пояс	Администраторы, локальная служба
Создать файл страницы	Администраторы
Создание символическое обозначение объекта	Никто
Создать постоянные совместно используемые объекты	Никто
Ограничить доступ к данному компьютеру из сети	Анонимный вход, гостевая группа
Запретить вход в качестве пакетного задания	Анонимный вход, гостевая группа
Запретить вход в качестве службы	Никто
Запретить локальный вход	Анонимный вход, гостевая группа
Запретить вход через службы удаленного рабочего стола	Анонимный вход, гость
Разрешить использование компьютера и учетных записей пользователей для делегирования	Никто
Принудительно завершать работу с удаленного компьютера	Администраторы
Создавать журналы безопасности	Локальная служба, сетевая служба
Увеличить приоритет планирования	Администраторы
Загружать и удалять драйверы устройств	Администраторы
Изменить метку объекта	Никто
Изменить значения среды микропрограммы	Администраторы
Выполнять задачи техобслуживания устройства	Администраторы

Задать параметры единого процесса	Администраторы
Отключить компьютер от установочной станции	Администраторы
Восстановить файлы и каталоги	Администраторы
Выключить систему	Администраторы
Синхронизировать служебные данные каталогов	Никто
Получить контроль файлов и других объектов	Администраторы

4.6.10 Экранная заставка

– Активировать защищенную паролем заставку и определить время ожидания:
Политики локального компьютера -> Конфигурация пользователя -> Шаблоны администратора -> Панель управления -> Персонализация

Активировать заставку	Активирован
Защитить заставку паролем	Активирован
Время ожидания заставки	1800 секунд

4.6.11 Активировать настройки требований к паролям

– Включение требований к паролям обеспечит соответствие паролей пользователей минимальным требованиям

Политики локального компьютера -> Параметры Windows -> Параметры безопасности -> Политика учетных записей -> Политика паролей

Вести журнал паролей	Хранить 10 последних паролей
Максимальный срок действия пароля	90 дней
Минимальный срок действия пароля	1 день
Минимальная длина пароля	10 символов
Пароль должен соответствовать требованиям сложности	Активирован
Хранить пароль с использованием обратимого шифрования для всех пользователей в домене	Отключен

4.6.12 Отключить службы Windows, не обязательные для функционирования

– Отключение служб Windows, не обязательных для функционирования, обеспечивает более высокий уровень безопасности и сводит к минимуму количество точек воздействия.

Служба шлюза на уровне приложения	Отключен
Диспетчер приложений	Отключен
Браузер компьютера	Отключен
Клиент отслеживания изменившихся связей	Отключен
Функция обнаружения поставщика узла	Отключен
Функция обнаружения ресурсов публикации	Отключен

Доступ к устройствам интерфейса пользователя	Отключен
Общий доступ к подключению к Интернету (ICS)	Отключен
Диспетчер обнаружения топологии канального уровня	Отключен
Планировщик классов мультимедиа	Отключен
Автономные файлы	Отключен
Диспетчер автоматических подключений удаленного доступа	Отключен
Диспетчер подключения удаленного доступа	Отключен
Маршрутизация и удаленный доступ	Отключен
Обнаружение оборудования оболочки	Отключен
Консольный помощник специального управления	Отключен
Обнаружение SSDP	Отключен

4.6.13 Учетные записи пользователей операционной системы Windows

Учетные записи пользователей операционной системы Windows должны быть защищены сложными паролями.
Серверы обычно управляются и обслуживаются с помощью учетных записей администратора Windows, убедитесь что учетные записи администратора защищены надежными паролями.

Пароли должны содержать символы из трех следующих категорий:
- Символы верхнего регистра европейских языков (От A до Z, с диакритическими знаками, греческие и кириллические символы)
- Символы нижнего регистра европейских языков (от a до z, эсцет, с диакритическими знаками, греческие и кириллические символы)
- Базовые 10 цифр (от 0 до 9)
- Не буквенно-цифровые символы: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Любой символ Unicode, попадающий в категорию буквенного, но не являющийся символом верхнего или нижнего регистра. Это включает символы Unicode из азиатских языков.

Использование блокировки учетной записи Windows для предотвращения успешных попыток взлома пароля.
Windows8.1 Базовые рекомендации безопасности 10/15/15:
- 10 неудачных попыток входа
- Блокировка 15 минут
- Сброс счетчиков в течение 15 минут

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Политика учетной записи -> Политика блокировки учетной записи

Продолжительность блокировки учетной записи	Продолжительность блокировки учетной записи

Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа	Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа
Сброс счетчика блокировки через	Сброс счетчика блокировки через

– Убедитесь, что пароль сервера по умолчанию и пароль операционной системы Windows заменены новыми надежными паролями.

4.6.14 Включить брандмауэр на сервере

▸ Включить связь стандартного порта BVMS в соответствии с портами BVMS.

Замечание!
См. документацию по BVMS, чтобы настроить и использовать порт соответствующим образом. Не забудьте еще раз проверить параметры обновления микропрограммы или ПО.

4.7 Усиление безопасности клиентов Windows

4.7.1 Рабочие станции Windows

Настольные операционные системы Windows, используемые для клиентских приложений BVMS, таких как BVMS, Operator Client или Configuration Client, устанавливаются за пределами защищенного места. Рабочие станции должны быть усилены для защиты видеоданных, документов и других приложений от несанкционированного доступа. Необходимо применить или проверить следующие настройки.

4.7.2 Рекомендуемые параметры оборудования рабочей станции Windows

– Установите пароль BIOS/ UEFI, чтобы запретить запуск альтернативных операционных систем.
– С целью предотвращения передачи данных клиенту USB-порты, а также CD и DVD-приводы должны быть отключены. Кроме того, неиспользуемые порты NIC также следует отключить.

4.7.3 Рекомендуемые настройки безопасности для операционной системы Windows

– Рабочая станция должна быть частью домена Windows.
  Интеграция рабочей станции в домен Windows позволит централизованно управлять параметрами безопасности.
– Обновления Windows
  . Следите за последними исправлениями и обновлениями ПО Windows.
– Установка антивирусного ПО
  Установите антивирусное и антишпионское ПО и регулярно обновляйте его.

4.7.4 Рекомендуемые настройки для операционной системы Windows

Следующие параметры локальной групповой политики — это рекомендуемые групповые параметры в серверной операционной системе Windows. Чтобы изменить политики локального компьютера (LCP) по умолчанию, используйте редактор локальной групповой политики (LGP).
Вы можете открыть редактор LGP с помощью командной строки или используя консоль управления Microsoft (MMC).

Чтобы открыть редактор LGP из командной строки:

▸ нажмите **Пуск**, в поле поиска **Пуск** введите **gpedit.msc** и нажмите Enter.

Чтобы открыть редактор LGP как встраиваемый модуль MMC:

1. нажмите **Пуск**, в поле поиска **Пуск** введите **mmc** и нажмите клавишу Enter.
2. В диалоговом окне **добавления и удаления встраиваемых модулей** нажмите **редактор объектов групповой политики** и нажмите кнопку **добавить**.
3. В диалоговом окне **выберите объект групповой политики** нажмите **обзор**.
4. Нажмите **компьютер** для изменения объекта локальной групповой политики и нажмите кнопку **пользователи** для изменения объектов групповой политики администратора, не администратора и пользователя.
5. Нажмите **Готово**

4.7.5 Активировать контроль учетных записей на сервере

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Локальная политика -> Настройки безопасности

Контроль учетных записей: режим одобрения администратором для встроенной учетной записи администратора	Активирован
Контроль учетных записей: позволить приложениям UIAccess запрашивать расширение прав доступа без использования безопасного рабочего стола	Отключен
Контроль учетных записей: запрос на расширение прав администратором в режиме одобрения администратором	Запрос разрешения
Контроль учетных записей: запрос на расширение прав для обычных пользователей	Запрос учетных данных в системе безопасного рабочего стола
Контроль учетных записей: обнаружение установки приложений и запрос расширения прав	Активирован
Контроль учетных записей: расширять права только для подписанных и проверенных исполняемых файлов	Отключен
Контроль учетных записей: все администраторы работают в режиме одобрения администратором	Активирован
Контроль учетных записей: переключение в режим безопасного рабочего стола при выполнении запроса на расширение прав	Активирован
Контроль учетных записей: виртуализация ошибок записи в файл и реестр в пользовательское расположение	Активирован

Политики локального компьютера -> Конфигурация компьютера -> Шаблоны администратора -> Компоненты Windows -> Интерфейс учетных данных пользователя

Нумеровать учетные записи администратора при расширении прав	Отключен

4.7.6 Отключение автозапуска

Политики локального компьютера -> Конфигурация компьютера -> Шаблоны администратора -> Компоненты Windows -> Политика автозапуска

Отключить автозапуск	Включить все диски

По умолчанию для автозапуска	Флажок установлен, не выполнять команды автозапуска
Отключить автозапуск для недисковых устройств	Активирован

4.7.7 Внешние устройства

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Локальная политика -> Настройки безопасности

Устройства: разрешить отстыковку без выполнения входа	Отключен
Устройства: разрешено форматирование и извлечение подключаемых устройств	Администраторы
Устройства: не позволять пользователям устанавливать драйверы принтера	Активирован
Устройства: предоставлять доступ к CD-ROM только пользователям, выполнившим вход на местном уровне	Активирован
Устройства: предоставлять доступ к дискетному приводу только пользователям, выполнившим вход на местном уровне	Активирован

4.7.8 Конфигурация назначения прав пользователя

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Назначение прав пользователя

Доступ к диспетчеру учетных данных в качестве надежного оператора	Никто
Доступ к компьютеру через сеть	Проверенные пользователи
Действовать как часть операционной системы	Никто
Добавить рабочие станции к домену	Никто
Разрешить вход через службы удаленного рабочего стола	Администраторы, пользователи удаленного рабочего стола
Изменить время системы	Администраторы
Изменить часовой пояс	Администраторы, локальная служба
Создать файл страницы	Администраторы
Создание символическое обозначение объекта	Никто
Создать постоянные совместно используемые объекты	Никто
Ограничить доступ к данному компьютеру из сети	Анонимный вход, гостевая группа
Запретить вход в качестве пакетного задания	Анонимный вход, гостевая группа

Запретить вход в качестве службы	Никто
Запретить локальный вход	Анонимный вход, гостевая группа
Запретить вход через службы удаленного рабочего стола	Анонимный вход, гость
Разрешить использование компьютера и учетных записей пользователей для делегирования	Никто
Принудительно завершать работу с удаленного компьютера	Администраторы
Создавать журналы безопасности	Локальная служба, сетевая служба
Увеличить приоритет планирования	Администраторы
Загружать и удалять драйверы устройств	Администраторы
Изменить метку объекта	Никто
Изменить значения среды микропрограммы	Администраторы
Выполнять задачи техобслуживания устройства	Администраторы
Задать параметры единого процесса	Администраторы
Отключить компьютер от установочной станции	Администраторы
Восстановить файлы и каталоги	Администраторы
Выключить систему	Администраторы
Синхронизировать служебные данные каталогов	Никто
Получить контроль файлов и других объектов	Администраторы

4.7.9 Экранная заставка

– Активировать защищенную паролем заставку и определить время ожидания:
Политики локального компьютера -> Конфигурация пользователя -> Шаблоны администратора -> Панель управления -> Персонализация

Активировать заставку	Активирован
Защитить заставку паролем	Активирован
Время ожидания заставки	1800 секунд

4.7.10 Активировать настройки требований к паролям

– Включение требований к паролям обеспечит соответствие паролей пользователей минимальным требованиям

Политики локального компьютера -> Параметры Windows -> Параметры безопасности -> Политика учетных записей -> Политика паролей

Вести журнал паролей	Хранить 10 последних паролей
Максимальный срок действия пароля	90 дней
Минимальный срок действия пароля	1 день
Минимальная длина пароля	10 символов

Пароль должен соответствовать требованиям сложности	Активирован
Хранить пароль с использованием обратимого шифрования для всех пользователей в домене	Отключен

4.7.11 Отключить службы Windows, не обязательные для функционирования

– Отключение служб Windows, не обязательных для функционирования, обеспечивает более высокий уровень безопасности и сводит к минимуму количество точек воздействия.

Служба шлюза на уровне приложения	Отключен
Диспетчер приложений	Отключен
Браузер компьютера	Отключен
Клиент отслеживания изменившихся связей	Отключен
Функция обнаружения поставщика узла	Отключен
Функция обнаружения ресурсов публикации	Отключен
Доступ к устройствам интерфейса пользователя	Отключен
Общий доступ к подключению к Интернету (ICS)	Отключен
Диспетчер обнаружения топологии канального уровня	Отключен
Планировщик классов мультимедиа	Отключен
Автономные файлы	Отключен
Диспетчер автоматических подключений удаленного доступа	Отключен
Диспетчер подключения удаленного доступа	Отключен
Маршрутизация и удаленный доступ	Отключен
Обнаружение оборудования оболочки	Отключен
Консольный помощник специального управления	Отключен
Обнаружение SSDP	Отключен

4.7.12 Учетные записи пользователей операционной системы Windows

Учетные записи пользователей операционной системы Windows должны быть защищены сложными паролями.
Серверы обычно управляются и обслуживаются с помощью учетных записей администратора Windows, убедитесь что учетные записи администратора защищены надежными паролями.

Пароли должны содержать символы из трех следующих категорий:
– Символы верхнего регистра европейских языков (От A до Z, с диакритическими знаками, греческие и кириллические символы)

- Символы нижнего регистра европейских языков (от a до z, эсцет, с диакритическими знаками, греческие и кириллические символы)
- Базовые 10 цифр (от 0 до 9)
- Не буквенно-цифровые символы: ~!@#$%^&*_-+=`|\(){}[]:;"'<>,.?/
- Любой символ Unicode, попадающий в категорию буквенного, но не являющийся символом верхнего или нижнего регистра. Это включает символы Unicode из азиатских языков.

Использование блокировки учетной записи Windows для предотвращения успешных попыток взлома пароля.
Windows8.1 Базовые рекомендации безопасности 10/15/15:
- 10 неудачных попыток входа
- Блокировка 15 минут
- Сброс счетчиков в течение 15 минут

Политики локального компьютера -> Конфигурация компьютера -> Параметры Windows -> Параметры безопасности -> Политика учетной записи -> Политика блокировки учетной записи

Продолжительность блокировки учетной записи	Продолжительность блокировки учетной записи
Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа	Учетная запись блокируется на 15 минут в случае 10 неудачных попыток входа
Сброс счетчика блокировки через	Сброс счетчика блокировки через

- Убедитесь, что пароль сервера по умолчанию и пароль операционной системы Windows заменены новыми надежными паролями.
- Отключите неиспользуемые учетные записи операционной системы Windows.
- Отключите удаленный доступ к рабочему столу клиентской рабочей станции.
- Запускайте рабочую станцию без прав администратора в целях избежания изменения параметров системы стандартным пользователем.

4.7.13 Активируйте брандмауэр на рабочей станции

▸ Включить связь стандартного порта BVMS в соответствии с портами BVMS.

Замечание!
См. документацию по BVMS, чтобы настроить и использовать порт соответствующим образом. Не забудьте еще раз проверить параметры обновления микропрограммы или ПО.

4.8 Защита доступа к сети

В настоящий момент многие малые и средние системы IP-видеонаблюдения размещены в существующей сетевой инфраструктуре клиентов как «очередное ИТ-приложение». Несмотря на преимущества в отношении цены и обслуживания, такой тип размещения также подвергает систему нежелательным угрозам, в том числе внутренним. Необходимо принять соответствующие меры и избегать ситуаций, когда видеозапись события попадает в Интернет или социальные сети. Такие ситуации могут не только нарушить конфиденциальность, но и в потенциале нанести вред компании.

Существует две основные технологии создания сети-в-сети. Какая именно будет выбрана создателями ИТ-инфраструктуры во многом зависит от существующей сетевой инфраструктуры, имеющегося сетевого оборудования и требуемых возможностей и топологии сети.

4.8.1 VLAN: виртуальная сеть LAN

Виртуальная сеть LAN создается путем разделения LAN на несколько сегментов. Сегментация сети осуществляется с помощью конфигурации сетевого коммутатора или роутера. VLAN имеет следующее преимущество: потребности в ресурсах могут быть удовлетворены без изменений в сетевых подключениях устройства.
Качество схем обслуживания, применяемых к конкретных сегментам, например, для видеонаблюдения, может повысить не только уровень безопасности, но и производительности.

Сети VLAN внедряются на канальном уровне сети (уровень OSI 2) и обеспечивают аналогию созданию IP-подсетей (см. *Назначение IP-адресов, Страница 8*) на уровне сети (уровень OSI 3).

4.8.2 VPN: виртуальная частная сеть

Виртуальная частная сеть — это отдельная (частная) сеть, которая часто основывается на нескольких общественных сетях или Интернете. Существует множество протоколов для создания сети VPN, которая обычно представляет собой тоннель, по которому перемещаются защищенные данные. Виртуальные частные сети можно создать в виде двухточечных туннелей, всеобщих подключений или многопортовых подключений. Сеть VPN может быть развернута с шифрованной связью или просто использовать безопасное соединение в рамках самой VPN.

VPN может использоваться для подключения к удаленным сайтам через подключения глобальной сети (WAN), но при этом также обеспечивать конфиденциальность и повышать уровень безопасности локальной сети (LAN). Поскольку виртуальная частная сеть действует как отдельная сеть, все устройства, добавленные к VPN, будут работать гладко, как если бы они были частью обычной сети. VPN не только обеспечивает дополнительный уровень защиты для системы наблюдения, но и предлагает дополнительное преимущество сегментации бизнес-данных производственной сети и видеоданных.

Замечание!
Если это применимо, VPN или VLAN повышают уровень безопасности системы видеонаблюдения в существующей ИТ-инфраструктуре.

Помимо зашиты системы от несанкционированного доступа в совместно используемой ИТ-инфраструктуре, необходимо уделить внимание тому, кто имеет право подключаться к этой сети вообще.

4.8.3 Отключение неиспользуемых портов коммутаторов

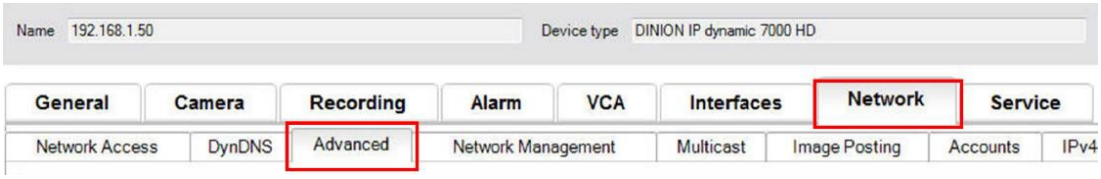
Отключение неиспользуемых сетевых портов обеспечивает невозможность доступа к сети несанкционированных устройств. Это снижает риск чьих-либо попыток получить доступ к подсети безопасности с помощью подключения своего устройства к коммутатору или неиспользуемому сетевому разъему. Возможность отключения конкретных портов является стандартным решением для управляемых коммутаторов, низкозатратным и подходящим для корпоративного применения.

4.8.4 802. 1 x защищенные сети

Все IP-видеоустройства Bosch можно настроить как клиенты 802.1x. Эта возможность позволяет им проходить проверку подлинности для подключения к серверу RADIUS и участия в защищенной сети. Прежде чем размещать видеоустройства в безопасной сети, вам потребуется прямое подключение к видеоустройству с ноутбука специалиста технической поддержки для ввода учетных данных, как указано ниже.

Сервисы 802.1x можно легко настроить с помощью Configuration Manager.

1. В Configuration Manager выберите желаемое устройство.
2. Выберите вкладку **Сеть**, затем выберите **Дополнительно**



3. Откройте часть страницы **802.1x**.
4. В раскрывающемся списке **802.1x выберите Вкл.**
5. Введите действительный **Удостоверение** и **Пароль.**
6. Сохраните изменения.
7. Отключите и разместите устройства в защищенной сети.

Замечание!
Сам по себе 802.1x не обеспечивает безопасное соединение между запрашивающим устройством и сервером проверки подлинности.
В результате имя пользователя и пароль могут быть «украдены» из сети. 802.1x может использовать EAP-TLS для обеспечения безопасной связи.

Расширяемый протокол проверки подлинности — безопасность транспортного уровня
Расширяемый протокол проверки подлинности (EAP) обеспечивает поддержку нескольких методов проверки подлинности. Безопасность транспортного уровня (TLS) обеспечивает взаимную проверку подлинности, согласование с целостно-защищенным набором шифров и обмен ключами между двумя конечными точками. EAP-TLS поддерживает взаимную проверку подлинности сертификатов и формирование ключей. Другими словами, EAP-TLS включает процесс, в котором и сервер, и клиент отправляют друг другу сертификат.

Замечание!
Обратитесь к специальной технической белой книге *Проверка подлинности сети — 802.1x — обеспечение безопасности сетевой периферии*, доступной в каталоге продукции Bosch Security Systems по ссылке:
http://resource.boschsecurity.com/documents/WP_802.1x_Special_enUS_22335867275.pdf.

5 Безопасная работа

5.1 Разделение сети

Где это возможно, устройство должно работать в отдельной сети с ограниченным доступом (например, можно использовать виртуальную локальную сеть (VLAN)), чтобы ограничить широковещательный трафик и защитить устройства от сетевых атак.

5.2 Безопасное хранение ключей в аппаратном хранилище

Лучший способ защитить закрытые ключи сертификатов — это хранить их на аппаратном компоненте, также называемом аппаратным хранилищем. Это микропроцессоры, защищающие закрытые ключи от несанкционированного доступа, даже если устройство физически вскрыто для получения доступа.
В камерах Bosch такие ключи хранятся в отдельном криптопроцессоре или защищенном элементе (SE). Оба решения обеспечивают безопасное хранение, а также криптографические функции, которые никогда не раскроют закрытые ключи в расположениях или памяти, где они потенциально могут быть извлечены.
На рабочих станциях и серверах обычно имеется доверенный платформенный модуль (TPM). Где это возможно, криптографические библиотеки и функции необходимо настроить для использование хранилища TPM.

5.3 Уникальные сертификаты устройств

Хотя самозаверяющий сертификат по умолчанию обычно доступен на каждом устройстве с поддержкой протоколов TLS или HTTPS, одного лишь его недостаточно для проверки подлинности, поскольку он не защищает от атак посредника (MITM).

Если устройства размещены в среде, где для проверки подлинности каждого отдельного IP-видеоустройства требуются дополнительные этапы, новые сертификаты и частные ключи могут быть созданы и загружены на эти видеоустройства. Новые сертификаты можно получить у органа сертификации или их можно создать, например, с помощью комплекта инструментов для работы с OpenSSL.

Если устройства используются в общественных сетях, рекомендуется получить сертификаты от общественного управления по сертификатам, или получить подпись такого органа на сертификатах; такой орган также может подтвердить происхождение и действительность — другими словами подлинность — сертификата устройства.

Уже некоторое время все камеры Bosch поставляются с предустановленным уникальным сертификатом устройства и закрытым ключом, полученным из корневого сертификата Bosch и установленным в безопасной производственной среде. Этот сертификат доказывает, что камера является первоначально изготовленным устройством Bosch. Этот сертификат используется для автоматического подключения по протоколу HTTPS и может применяться для идентификации и проверки подлинности устройства путем верификации цепочки сертификатов вплоть до корневого сертификата Bosch.

Замечание!
Сертификаты следует использовать для авторизации одного устройства. Рекомендуется создать конкретный сертификат для каждого устройства на основе главного сертификата.

Наиболее безопасным вариантом развертывания сертификата является генерация запроса на подписание сертификата (CSR) на устройстве и запрос сертификата у внутреннего или внешнего центра сертификации.
При запросе на подписание сертификата устройство хранит закрытый ключ во внутренней среде и раскрывает для подписания центром сертификации только остальную часть сертификата. Закрытый ключ безопасно хранится в защищенном элементе (SE) камеры или, например, в доверенном платформенном модуле (TPM) устройства.
Поэтому, если на устройстве доступна функция CSR, она должна быть выбрана в качестве предпочтительного способа создания сертификата.

Сертификаты можно загрузить на устройство либо с помощью веб-страницы видеоустройства, либо с помощью Configuration Manager.

Загрузка сертификатов с помощью веб-страницы устройства
Сертификаты можно загрузить с использованием веб-страницы видеоустройства.
На веб-странице устройства, на странице **Сертификаты** можно удалять и добавлять новые сертификаты, а также задавать параметры их использования.

Загрузка сертификатов с помощью Configuration Manager
В Configuration Manager сертификаты можно легко загружать на отдельные устройства или на несколько устройств одновременно.
Чтобы загрузить сертификаты:
1. В Configuration Manager выберите одно или несколько устройств.
2. Нажмите правой кнопкой и выберите **Отправка файла**, затем нажмите **Сертификат SSL...**.
   Откроется окно Windows Explorer для выбора сертификата для загрузки.

Для небольших систем Configuration Manager имеет вспомогательную функцию **MicroCA**, которая позволяет создавать или использовать корневой CA и получать из него сертификаты устройств, а также использовать его для подписания запросов на подписание сертификатов устройств, в том числе для нескольких устройств одновременно. Подробнее см. в руководстве пользователя Configuration Manager.

См.
– *Установление доверия с помощью сертификатов, Страница 50*

5.4 Проверка файлов журнала

Мониторинг файлов журнала является важной частью анализа безопасности или процедур технического обслуживания. Регулярный просмотр файлов журнала позволяет выявить проблемы с конфигурацией или с безопасностью, такие как ложные входы в систему.
Для анализа файлов журнала и их длительного хранения рекомендуется отправлять файлы журнала устройства на сервер syslog или в систему сбора и корреляции событий (SIEM), поскольку камера выделяет для ведения журнала на устройстве фиксированный объем памяти, при заполнении которого старые журналы перезаписываются.

5.5 Система SIEM

Система сбора и корреляции событий (SIEM) используется для сбора и анализа информации с различных устройств и систем. Устройства можно интегрировать в систему SIEM, отправляя журналы по протоколу syslog. Анализ этих журналов помогает в техническом обслуживании и обнаружении ошибок конфигурации или атак на устройство (например, ложных входов в систему).

5.6 PKI

Инфраструктура открытых ключей (PKI) — это системы, необходимые для создания цифровых сертификатов и управления ими. Для подключений по протоколу HTTPS, проверки подлинности в сети по стандарту 802.1x, проверки подлинности пользователей с помощью сертификатов и работы других функций шифрования на устройство могут устанавливаться настраиваемые сертификаты.

5.7 AD FS

Active Directory Federation Services (AD FS) — это служба Microsoft, позволяющая выполнять проверку подлинности в локальном домене Active Directory (с помощью сервера AD FS) или в облаке Azure Cloud. Помимо локальной проверки подлинности пользователей с помощью паролей или сертификатов, с помощью AD FS возможна интеграция устройств в домен Active Directory для централизованной проверки подлинности и управления доступом.

5.8 Безопасная работа IP-камер

5.8.1 Установление доверия с помощью сертификатов

Все IP-камеры Bosch с версией микропрограммы 6.10 или более поздней используют хранилище сертификатов, которое можно найти в меню **Обслуживание** конфигурации камеры.

Конкретные сертификаты серверов, сертификаты клиентов и доверенные сертификаты могут быть добавлены в хранилище.

Чтобы добавить сертификат в хранилище:

1. На веб-странице устройства перейдите на страницу **Конфигурация**.
2. Выберите меню **Обслуживание** и подменю **Сертификаты**.
3. В разделе **Список файлов** выберите **Добавить**.
4. Загрузите желаемые сертификаты.
   После завершения загрузки сертификаты отображаются в разделе **Список использования**.
5. В разделе **Список использования** выберите желаемый сертификат.
6. Для активации использования сертификатов камеру необходимо перезагрузить. Для перезагрузки камеры нажмите **Установить**.

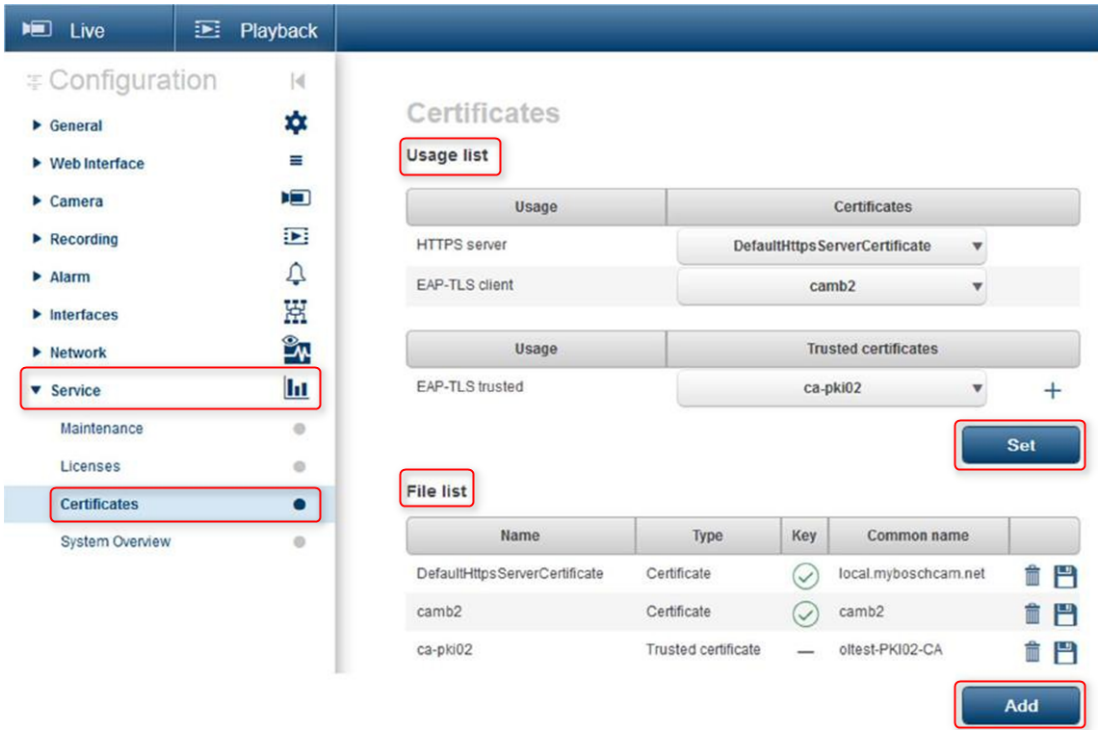


Рис. 5.1: Пример: сертификаты EAP/TLS хранятся в камере Bosch с версией микропрограммы 6.11.

Сертификаты принимаются в формате *.pem, *.cer или *.crt и должны быть закодированы в Base64. Их можно загрузить единым файлом или разделить на файлы сертификатов и ключей и загрузить в этом порядке как отдельные файлы для последующего автоматического объединения.

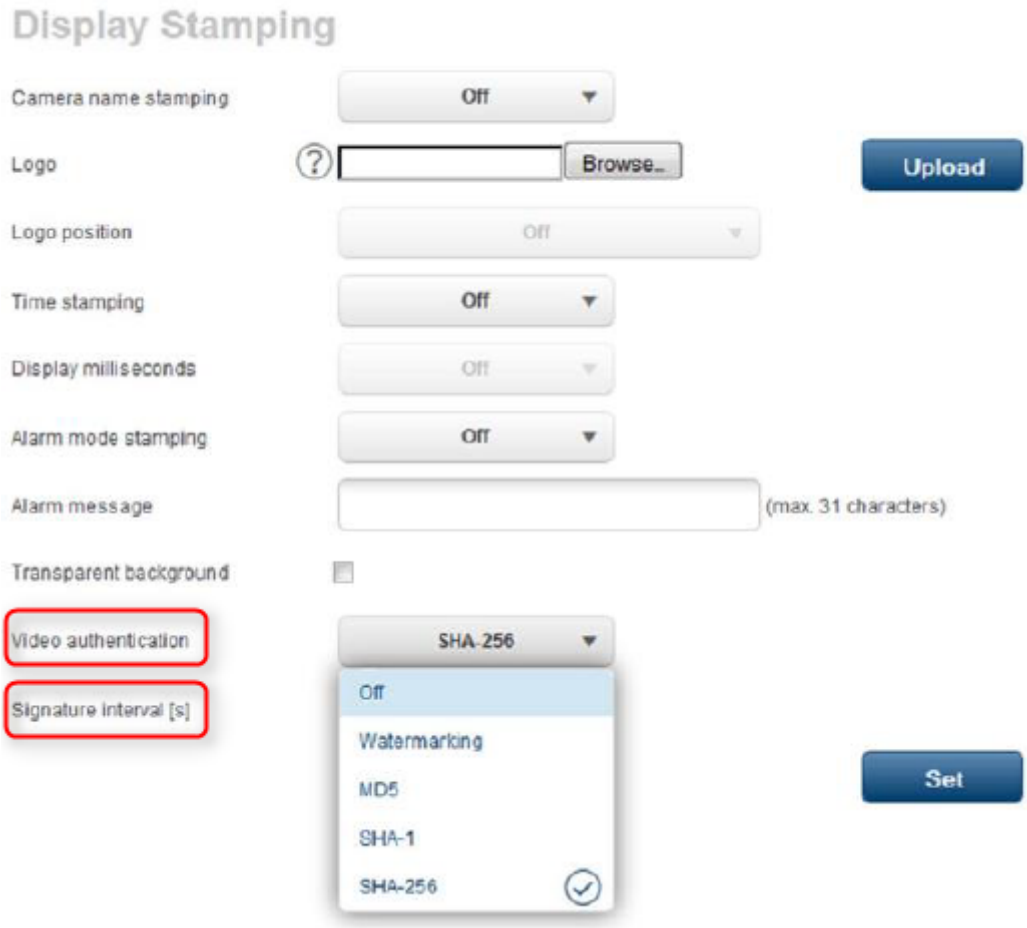
Начиная с версии микропрограммы 6.20, поддерживаются частные защищенные паролем ключи PKCS#8 (шифрованные с помощью AES), которые должны быть загружены в формате *.pem и закодированы в Base64.

5.8.2 Функция установления подлинности видеоизображения

Как только устройства в системе будут должным образом защищены и пройдут проверку подлинности, стоит также следить за видеоданными, получаемыми с них. Этот метод называется проверкой подлинности видео.
Проверка подлинности видео связана только с методами проверки подлинности видео. Проверка подлинности видео никаким образом не связана с передачей видео или данных. До выхода микропрограммы 5.9 водяные знаки наносились на видеопоток с помощью простого алгоритма контрольной суммы. При работе с базовым нанесением водяных знаков нет смысла использовать сертификаты или шифрование. Контрольная сумма — это базовое измерение «постоянности данных» файла, которое подтверждает целостность файла.
Чтобы настроить проверку подлинности видео, например, в веб-браузере:

1. Перейдите в меню **Общие** и выберите **Надписи на экране**.
2. В раскрывающееся меню **Проверка подлинности видео** выберите нужный вариант: Микропрограмма версии 5.9 и более поздние версии обеспечивают три параметра установления подлинности видеоизображений помимо классических водяных знаков:
   – MD5: краткое сообщение, производящее 128-битовое хеш-значение.

- SHA-1: разработанный управлением национальной безопасности США федеральный стандарт обработки информации, опубликованный Национальным институтом стандартов и технологии США. SHA-1 производит 160-битовое хеш-значение.
- SHA-256: SHA-256 формирует практически уникальное 256-битовое (32-байтовое) хеш-значение фиксированного размера.



Замечание!
Хеш является необратимой функцией, ее невозможно расшифровать.

При использовании установления подлинности видеоизображений каждый пакет видеопотока хэшируется. Эти хэши встроены в поток видео и хэшируются сами вместе с видеоданными. Это гарантирует целостность содержания потока.

Хэши регулярно подписываются с определенным интервалом с использованием частного ключа хранящегося в модуле TPM устройства сертификата. Запись по тревоге и изменения блоков в записях iSCSI закрываются подписью в целях обеспечения непрерывной подлинности видео.

Замечание!
Расчет цифровой подписи требует вычислительной мощности, которая может повлиять на общую производительность камеры, если его проводить слишком часто. Поэтому следует выбрать приемлемый интервал.

Так как хэши и цифровые подписи внедряются в поток видео, они также сохраняются в записи, позволяя устанавливать подлинность видеоизображений также для воспроизведения и экспорта.

6 Управление обновлениями для системы безопасности

Перед первым использованием устройства установите самую актуальную версию ПО. Для обеспечения оптимальных функциональных возможностей, совместимости, производительности и безопасности регулярно обновляйте ПО в течение всего срока эксплуатации устройства. Следуйте инструкциям в документации к продукту в отношении обновлений ПО.

Более подробную информацию можно получить по следующим ссылкам:

– общие сведения: https://www.boschsecurity.com/xc/en/support/product-security/
– рекомендации по безопасности, а именно список обнаруженных уязвимых мест и предлагаемых решений: https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html

Компания Bosch не берет на себя никакой ответственности за какой-либо ущерб, вызванный эксплуатацией ее продуктов при использовании устаревшего ПО.

Последние версии микропрограммного и программного обеспечения можно найти в центре загрузки Bosch Security and Safety Systems:
https://downloadstore.boschsecurity.com/

Благодаря сервису Remote Alert пользователи могут получать по электронной почте уведомления о доступных обновлениях микропрограммного обеспечения для устройств, подключенных к порталу Remote Portal.

Более полные пакеты загрузки распространяются через каталог продуктов Bosch Security and Safety Systems:
https://www.boschsecurity.com

7 Контроль безопасности

Поскольку требования постоянно меняются, никогда невозможно гарантировать полную безопасность. Поэтому компания Bosch разработала структурированный процесс управления уязвимостями и инцидентами для профессионального управления потенциальными уязвимостями продуктов и происшествиями.

Для нас очень важна профессиональная систематическая обработка сообщений об уязвимостях и прозрачность по отношению к нашему клиенту. Именно поэтому мы изучаем все сообщения об уязвимостях. Мы оцениваем уязвимости продукта по системе Common Vulnerability Scoring System (CVSS). Система CVSS — это бесплатный открытый отраслевой стандарт для оценки серьезности уязвимостей компьютерных систем. Баллы рассчитываются по формуле, учитывающей несколько показателей, которые позволяют примерно оценить легкость и последствия использования уязвимости. Уязвимость может получить от 0 до 10 баллов, где 10 означает самую серьезную угрозу.

Если наличие уязвимости подтверждается, мы информируем клиентов о выявленной уязвимости в продукте или решении, а также о методе ее устранения, публикуя советы по безопасности. Сведения, содержащиеся во всех советах по безопасности:

- Описание уязвимости со ссылкой на базу данных Common Vulnerabilities and Exposures (CVE) и оценкой CVSS.
- Идентификаторы известных затронутых продуктов и версий программного/аппаратного обеспечения.
- Информация о смягчающих факторах и обходных путях.
- График выхода и местонахождение доступных исправлений и других средств устранения.

Список опубликованных советов по безопасности можно найти на нашем веб-сайте https://www.boschsecurity.com/xc/en/support/product-security/security-advisories.html. Если вы считаете, что обнаружили уязвимость или иную проблему безопасности, связанную с продуктом или сервисом Bosch, свяжитесь со службой реагирования на инциденты в области безопасности продуктов Bosch (PSIRT): https://psirt.bosch.com.

8 Безопасная утилизация и вывод из эксплуатации

В определенный момент жизненного цикла вашего продукта или системы может возникнуть необходимость заменить или вывести из эксплуатации само устройство или его компонент. Поскольку устройство или компонент могут содержать конфиденциальную информацию, такую как учетные данные или сертификаты, обеспечьте полное и безопасное удаления таких данных.

Настройки большинства устройств можно сбросить до заводских.
На большинстве IP-камер и кодеров для этого можно использовать кнопку сброса. Если устройство не оснащено кнопкой сброса, воспользуйтесь функцией сброса до заводских настроек в веб-интерфейсе, прежде чем отключить устройство от сети.
Все пользователи и их пароли будут удалены, а настройки сброшены до заводских настроек по умолчанию. Все сертификаты и соответствующие ключи, которые хранились в модуле TPM или защищенном элементе, также будут удалены.

На других устройствах сброс до заводских настроек может выполняться по-другому. Надлежащие методы утилизации см. в инструкциях в соответствующей документации для пользователей.
На серверах и рабочих станциях также могут храниться сертификаты и учетные данные. Используйте надлежащие инструменты и методы для безопасного удаления такого рода данных при выводе устройств из эксплуатации или перед утилизацией.

Если устройства планируется перенести в другую установку, где могут использоваться другие учетные данные и сертификаты, их настройки также рекомендуется сбросить до заводских настроек по умолчанию.

Замечание!
Надлежащие методы утилизации см. в инструкциях в соответствующей документации для пользователей.

9 Дополнительная информация

Для получения дополнительной информации, а также скачивания программного обеспечения и документации перейдите на страницу соответствующего продукта в каталоге продуктов:
http://www.boschsecurity.com

Глоссарий

802.1x

Стандарт IEEE 802.1x предоставляет метод проверки подлинности и авторизации для сетей на основе IEEE 802. Проверка подлинности осуществляется через аутентификатор, который проверяет переданную информацию о проверке подлинности при помощи сервера проверки подлинности (см. RADIUS-сервер) и разрешает или отказывает в доступе к предлагаемым службам (LAN, VLAN или WLAN соответственно).

DHCP

Сокращение от "Dynamic Host Configuration Protocol"; протокол, использующий соответствующий сервер для динамического назначения IP-адресов и других параметров конфигурации компьютерам в сети (в Интернете или локальной сети)

HTTP

Сокращение от "Hypertext Transfer Protocol"; протокол передачи данных по сети

HTTPS

Сокращение от "Hypertext Transfer Protocol Secure"; протокол, обеспечивающий безопасную передачу данных между веб-сервером и веб-браузером

LAN

Local Area Network; локальная сеть. Сеть, соединяющая устройства в пределах ограниченной географической области.

ONVIF

Открытый форум по интерфейсу сетевого видео (Open Network Video Interface Forum). Глобальный стандарт для сетевых видеопродуктов. Устройства, соответствующие стандарту ONVIF, могут в режиме реального времени обмениваться видео- и аудиоданными, метаданными и информацией управления и обеспечивать автоматическое обнаружение и подключение к сетевым приложениям (например, к системам управления видео).

RADIUS-сервер

Сокращение от "Remote Authentication Dial-in User Service"; служба удаленной проверки подлинности пользователей, устанавливающих соединение по телефонным линиям, клиент-серверный протокол для аутентификации, авторизации и учета пользователей, устанавливающих соединение по телефонным линиям, в компьютерных сетях. RADIUS фактически является стандартом централизованной проверки подлинности соединений по телефонным линиям для модемов, ISDN, VPN, беспроводной LAN (см. 802.1x) и DSL.

RCP+

Протокол дистанционного управления — запатентованный протокол Bosch, использующий определенные статические порты для определения IP-видеоустройств Bosch и связи с ними

RTSP

Real Time Streaming Protocol. Сетевой протокол, позволяющий управлять непрерывной передачей аудио- и видеоданных или программного обеспечения по IP-сетям.

SNMP

Сокращение от "Simple Network Management Protocol"; простой протокол управления сетью, предназначенный для управления сетевыми компонентами

SSL

Secure Sockets Layer; устаревший протокол шифрования для передачи данных в IP-сетях (см. TLS).

TCP

Сокращение от Transmission Control Protocol (протокол управления передачей). Ориентированный на подключение протокол связи, используемый для передачи данных по IP-сети. Предлагает надежную передачу упорядоченных данных.

Telnet

Протокол эмуляции терминала. Протокол (и соответствующие программы) из набора протоколов IP для реализации интерфейса сетевого виртуального терминала.

TLS

Протокол Transport Layer Security. TLS 1.0 и 1.1 представляют собой стандартное развитие SSL 3.0 (см. SSL). В современных устройствах используются версии TLS 1.2 или 1.3

TTL

Сокращение от "Time-To-Live"; срок жизни — время существования пакета данных при передаче по станциям

UDP

User Datagram Protocol; Протокол без установления соединения, используемый для обмена данными по IP-сети. Протокол UDP более эффективен для передачи видеоданных, чем протокол TCP по причине более низких потерь.

VPN

Виртуальная частная сеть (VPN) реализует частную сеть в общедоступной сети, например в Интернете. Передача данных по сети VPN зашифрована и защищена от шпионажа.

Адрес IPv4

4-байтовое число, задающее уникальный номер хост-компьютера в Интернет. Обычно указывается в десятичной системе счисления, например, "209.130.2.193"

Глобальная сеть

Канал дальнего действия, используемый для расширения или объединения удаленных локальных сетей

Маска сети

Маска, в которой содержится информация о том, какая часть IP-адреса представляет собой адрес сети, а какая часть представляет собой хост-адрес. Обычно указывается в десятичной системе счисления, например, "255.255.255.192".

Многоадресная передача

Связь по сети между одним отправителем и несколькими получателями посредством распределения одного потока данных в самой сети по нескольким получателям в определенной группе. Требованием к многоадресной передаче является сеть, совместимая с такой передачей и использующая протоколы UDP и IGMP.

Пользовательская группа

Пользовательские группы используются для определения общих пользовательских атрибутов, например, разрешений, привилегий и приоритетов PTZ. Когда пользователь становится членом пользовательской группы, он автоматически наследует все атрибуты группы.

проверка подлинности

Процедура проверки подлинности видеопотока. Пользователь может запустить процедуру проверки подлинности. Если встречаются неподлинные данные, на экране появляется сообщение.

Усиление безопасности

Процесс повышения уровня безопасности системы путем использования только специального программного обеспечения, необходимого для ее работы, применения специальных настроек защиты и удаления программного обеспечения, без которого можно обойтись.

устройство

Аппаратный компонент, например камера, кодер/декодер, сетевой видеорегистратор, DiBos, аналоговый матричный коммутатор, мост ATM/POS.

Bosch Sicherheitssysteme GmbH
Robert-Bosch-Ring 5
85630 Grasbrunn
Germany
www.boschsecurity.com

Building solutions for a better life.

202302091957